Medizinische Fakultät
der
Universität Duisburg-Essen

Alfried Krupp von Bohlen und Halbach Krankenhaus Essen
Klinik für Neurologie mit klinischer Neurophysiologie

Die Patientendaten-Transfer-Zone in der Architektur der Integrierten Versorgung – dezentral organisiert

Inaugural - Dissertation
zur
Erlangung des Doktorgrades der
Naturwissenschaften in der Medizin
durch die Medizinische Fakultät
der Universität Duisburg-Essen

Vorgelegt von
Thomas Jäschke
aus Gelsenkirchen
2005

Dekan: Univ.-Prof. Dr. rer. nat. K.-H. Jöckel
1. Gutachter: Priv.-Doz. Dr. rer. nat. R. R. Diehl
2. Gutachter: Univ.-Prof. Dr. rer. pol. Dipl.-Volkswirt J. Wasem

Tag der mündlichen Prüfung: 10. April 2006

Inhaltsverzeichnis

1 Einleitung

Am 14. November 2003 wurde das „Gesetz zur Modernisierung der gesetzlichen Krankenversicherung“, kurz GMG im Deutschen Bundestag mit Zustimmung des Bundesrates beschlossen. Dort werden in Artikel 1 die Änderungen des Fünften Buches Sozialgesetzbuch (SGB V) und speziell in §140b (Finanzierung) dieses Gesetzes die Möglichkeiten der Verträge zur Integrierten Versorgung behandelt. Ein neuer Artikel des SGB V, nämlich § 291 Abs. 2a legt fest, dass die Krankenkassen dazu verpflichtet sind, die bisherige Krankenversichertenkarte zu einer elektronischen Gesundheitskarte zu erweitern. Die Details über die Ausgestaltung dieser Patientenchipkarte werden in § 291a SGB V geregelt.

Am 1. Januar 2004 in Kraft getreten, werden im GMG die rechtlichen Rahmenbedingungen für den flächendeckenden Einsatz von Gesundheitstelematik mittels der elektronischen Gesundheitskarte geschaffen. Es regelt detailliert die Zugriffsrechte auf die Patientendaten und bezeichnet die wichtigsten Telematikanwendungen, die mit der Gesundheitskarte realisiert werden sollen, darunter das elektronische Rezept und die Arzneimitteldokumentation.

Im Kern des GMG geht es also um die Einführung der elektronischen Gesundheitskarte, die einen verpflichtenden administrativen und einen freiwilligen medizinischen Teil haben. Der verpflichtende administrative Teil der Karte enthält die Vertragsinformationen, die bereits bisher auf der Krankenversichertenkarte gespeichert waren. Aber auch wesentliche Details des freiwilligen medizinischen Teils der elektronischen Gesundheitskarte werden in § 291a SGB V festgeschrieben. So muss die Karte für das Erheben, Verarbeiten und Nutzen von Notfalldaten geeignet sein.

Vordringliches Ziel ist es, durch den Einsatz der Gesundheitskarte und elektronischer Datennetze, „…Kosten einzusparen, die im Gesundheitswesen entstehen, weil Verwaltungsvorgänge durch die gängigen Mischlösungen aus elektro-

nischer Dokumentation und Papierdokumentation unnötig komplex werden.“(DIMDI 2005)

Für die Umsetzung der Vorgaben zur Einführung des Pflichtteils des GMG ist als Stichtag der 1. Januar 2006 genannt worden. Die aktuelle Situation lässt jedoch vermuten, dass außer in einigen Test- bzw. Modellregionen noch kein flächendeckender Einsatz möglich sein wird.

Die vorliegende Ausarbeitung beschäftigt sich mit einem konkreten Ausschnitt des umfassenden Marktes im Gesundheitswesen. Es geht um die Zusammenarbeit von Krankenhäusern untereinander. Hintergrund dafür sind die aktuellen und pragmatischen Anforderungen für eine Kommunikationsunterstützung im Rahmen der Integrierten Versorgung, die einerseits nicht im Pflichtteil des GMG behandelt werden und dennoch die angestrebte Lösungsarchitektur unterstützen oder sogar ergänzen soll.

Diese Überlegungen resultieren aus den Diskussionen der Vergangenheit, dass die elektronische Gesundheitskarte als Datenträger benutzt werden könnte. Dabei stellte man sich vor, dass sämtliche relevanten Informationen über den Gesundheitszustand des Patienten auf dieser Karte sicher gespeichert werden sollen. Mittlerweile hat sich heraus kristallisiert, dass zunächst lediglich das elektronische Rezept mit der Karte transportiert werden soll und gegebenenfalls die Notfalldaten des Patienten dort gespeichert werden. Der EU-Auslandskrankenschein wird in der ersten Ausgabephase der Karte lediglich auf die Rückseite gedruckt werden.

Die Speicherung sämtlicher Informationen von diversen Krankenhausaufenthalten und Daten niedergelassener Ärzte auf der Karte hat neben der benötigten hohen Speicherkapazität, die in der Diskussion vernachlässigt werden kann, den Nachteil, dass bei Verlust der Karte ohne eine zentrale Archivierung eine Rekonstruktion der Daten aus den verschiedenen Untersuchungen kaum oder nur mit erheblichen Aufwand möglich ist. Außerdem besteht grundsätzlich die

Möglichkeit durch nicht befugte Personen, die verschlüsselten Informationen auf der Karte zu entschlüsseln. Damit soll die Sicherheit der aktuellen Technologie nicht in Frage gestellt werden, jedoch ist es vorstellbar, dass in einigen Jahren andere Möglichkeiten und größere Rechnerkapazitäten zur Verfügung stehen, die eine Entschlüsselung möglich machen könnten. Dies ist bei Daten, die einer gesetzlichen Speicherung von 30 Jahren unterliegen, nicht auszuschließen, und die Information kann auch nach einigen Jahren diese Arbeit wert sein. Mögliche Versuche, die Daten für missbräuchliche Zwecke zu entschlüsseln, würden in diesem Fall weder protokolliert noch verhindert werden können.

Dagegen hat der nun aktuelle Ansatz, die eigentliche elektronische Patientenakte zentral zu speichern, aus sicherheitstechnischer Sicht, große Vorteile. Unerlaubte Zugriffe können entdeckt und durch geeignete Maßnahmen verhindert werden. Die zentrale Ablage erlaubt außerdem die rasche Anpassung der kryptologischen Verfahren.

Diese Problematik ist jedoch schon seit langem Diskussionsgegenstand. Einem Gutachten über die Informationstechnologien im Gesundheitswesen ist zu entnehmen (Lauterbach und Lindlar 1999):
„Mittelfristig wird es durch neue Speichermedien auch möglich werden, die gesamte Patientenakte auf einer Patientenkarte abzulegen. Dieses Konzept enthält die Möglichkeit, über die Patientenkarte die Information des Patienten zu transportieren, so dass nur befugte Angehörige der Gesundheitsberufe sich eine Kopie der Patientenakte schaffen können. Sicherheitskopien können dabei in einer zentralen Datenbank gelagert werden, die nur bei Verlust und in Notfällen genutzt werden kann.“

Nachteilig bei diesem Ansatz ist, dass diese zentralen Archive (in den vereinigten Staaten spricht man von CDR[1]; clinical data repository) aufgebaut und betrieben werden müssen. Der Datenaustausch muss standardisiert und die Zugriffe müssen protokolliert werden. Eine gesetzliche Plattform für den Betrieb

[1] s.a. Glossar

wird es nach derzeitigem Stand nicht geben, so dass eine Lösungsarchitektur dieses Szenario beschreibt und der Industrie lediglich einen Rahmen für die Umsetzung vorgibt. Die Bundesregierung will dadurch sicherstellen, dass eine ausreichende Flexibilität und Wettbewerbssituation erhalten bleibt. Sicher ist indes, dass die Gesundheitskarte eine zentrale Rolle in der Telematik spielen wird: „The electronic health card serves as the basis and thus also as a lead-in to other applications of telematics, as e.g. the electronic patient record." (Dietzel und Riepe 2004)

Unabhängig von der letztendlichen Architektur ist es erforderlich, zur Steigerung der Effizienz und der Qualität Informationen elektronisch auszutauschen. Offen bleibt aber dabei, welche Informationen ausgetauscht werden sollen, wie die Selektion der benötigten Daten erfolgt und auf welchen Weg die die Informationen die Institution verlassen.

Ziel ist es, die Architektur einer gemeinsamen Plattform zu definieren und die benötigten Komponenten und Verfahren zu konkretisieren. Dabei ist den heterogenen Systemumgebungen der jeweiligen Kommunikationspartner eine besondere Aufmerksamkeit zu schenken. Angestrebtes Ziel ist daher ein flexibler und gleichsam pragmatischer Lösungsansatz, der sich einerseits an bereits bekannten Rahmenkonzepten orientiert, andererseits auf der Idee der so genannten „best practices" basiert, welche dann als sinnvoll und sogar als notwendig betrachtet werden können, wenn keine konkreten Vorgaben vorhanden sind. Der Hintergrund dabei ist der, dass bekannte und praxistaugliche Verfahren und Komponenten zum Einsatz kommen.

Vorweg geschickt sei, dass die Betrachtungen in der vorliegenden Arbeit eine Gesamtübersicht geben und nicht den Anspruch haben, einem Techniker der IT-Sicherheit eine Detailbeschreibung der einzelnen Komponenten zu geben. Vielmehr sollen Betroffenen und Entscheidungsträgern der prinzipielle Aufbau erläutert und entsprechende damit zusammenhänge Fragestellungen behandelt werden.

Das Thema der Arbeit stammt direkt aus meinem täglichen Arbeitsumfeld. Durch die Diskussionen um die Anforderungen und Bedenken bei der Öffnung für den Datentransfer mit Externen mit IT-Leitern und Geschäftsführern von Krankenhäusern, haben sich viele Fragen ergeben, die nach und nach beantwortet werden konnten und in der Gesamtheit das vorliegende Konzept ausmachen.

Aus wirtschaftlicher Sicht wurde meist die Investitionssicherheit angesprochen. Die Realisierung dieser Architektur soll flexibel sein und pragmatisch umgesetzt werden können, ohne in eine Sackgasse hinsichtlich der gesetzlichen Anforderungen, die im ständigen Fluss sind, zu geraten.

Eine eher strategische Diskussion beruht auf der Tatsache des immer mehr durch große Unternehmen bestimmten Markts in der Gesundheitsbranche. Die geforderte Lösung soll nach Möglichkeit neutral sein und mit allen führenden Systemen der diversen Anbieter funktionieren.

Der Aspekt des Datenschutzes spielt natürlich eine große Rolle in der Betrachtung einer möglichen Kommunikationsplattform. Es muss größtmögliche Sicherheit hergestellt werden, welche aber die Kommunikation in Ihrer Anwendung nicht behindern soll. Eine umständliche Nutzung würde zu Akzeptanzproblemen führen.

Zusammengefasst bedeutet dies, dass eine Struktur zum sicheren Datenaustausch im Gesundheitswesen gefordert wird, welche herstellerunabhängig, sicherheitstechnisch unbedenklich und durch eine intuitive Benutzeroberfläche, nach Möglichkeit browserbasiert. Umgesetzt werden kann. Dabei muss die Gesundheitspolitik im Auge behalten werden, so dass sich diese Architektur in die wachsende Struktur im Gesamtkontext einpassen kann und schon jetzt pragmatisch und investitionssicher umgesetzt werden kann.

2 Anforderungen

Ein Krankenhaus strebt eine enge Zusammenarbeit mit anderen Einrichtungen des Gesundheitswesens an. Bereits bestehende Kooperationen sollen weiter verstärkt und durch optimierte Abläufe wirtschaftlicher gemacht werden (vgl. Beske et al. 1993). Unterstützt werden soll dies durch den Einsatz einer geeigneten Telematik-Plattform.

„Die Telematik-Plattform ermöglicht Krankenhäusern eine Spezialisierung auf medizinische Kernkompetenzen. Durch Kooperation mit anderen Krankenhäusern und niedergelassenen Ärzten kann Patienten das volle Leistungsspektrum in höherer Qualität als bisher angeboten werden. Außerdem fördert die Telematik-Plattform die intensive Zusammenarbeit mit niedergelassenen Ärzten und Zahnärzten, die dadurch als regelmäßige Einweiser gewonnen und gebunden werden können.“ (Rohleder et al. 2003)

Die wirtschaftlichen Aspekte liegen einerseits in der Einsparung von Kommunikations- und Versandkosten von patientenrelevanten Informationen und auf der anderen Seite in der Vermeidung bzw. Reduzierung von Doppeluntersuchungen bei gleichzeitiger Erhöhung der Qualität. Prof. Roland Trill (FH Flensburg) spricht in diesem Zusammenhang von „eHealth“, in welchem „jene Bereiche und Prozesse des Gesundheitswesens und der Medizin gefasst werden, die auf Internettechnologien zurückgreifen“ (Trill 2002). Ebenso sei das Stichwort Doppeluntersuchung genannt. In diesem Zusammenhang können bei rechtzeitigem Vorliegen von Information ebenfalls Einsparungen erzielt werden: „Fehlende, unvollständige, unstrukturierte oder verspätet eingehende Informationen verursachen Kommunikationsbrüche – diese Faktoren bedingen eine mühselige Beschaffung von Vorinformationen (Diagnosen, Vorbefunde) und gegebenenfalls Untersuchungen, die in Kenntnis der Vorbefunde aus medizinischen Gründen nicht hätten durchgeführt werden müssen. Effizienz und Qualität der Behandlung können dadurch erheblich beeinträchtigt werden“ (Boeske et al. 2003).

Der Datentransfer soll nach Möglichkeit ohne Medienbruch von einem Standort zum anderen stattfinden und dabei den Anforderungen an den Datenschutz gerecht werden. Ein Hauptaugenmerk ist jedoch auch auf die Praktikabilität zu setzen, so dass die Kosten für die Umsetzung durch den Nutzen gerechtfertig werden können und den Medizinern in ihrer Tagesroutine keinen erhöhten Aufwand bescheren.

Das konkret angedachte Szenario sieht so aus, dass Patienten zur Weiterbehandlung von einem Krankenhaus in eine Spezialklinik überwiesen werden. Die bereits vorliegenden Befunde und Untersuchungsmaterialien (z.B. EKG, Laborwerte, Herzkatheterfilm etc) sollen der Spezialklinik zur Weiterbehandlung zur Verfügung gestellt werden. Dazu müssen aus den jeweiligen Systemen Informationen gewonnen, für die Übertragung vorbereitet und entsprechend übermittelt werden. Die Daten stammen alle aus dem internen Krankenhausinformationssystem (KIS[2]) der überweisenden Einrichtung. Der Begriff KIS steht in diesem Zusammenhang für die tatsächliche Summe aller beteiligten Anwendungssysteme und nicht, wie häufig im Gesundheitswesen benutzt, als Bezeichnung des administrativen Systems allein. In der Regel werden jedoch Informationen zu dem Patienten aus diesem administrativen System sowie aus zusätzlich angeschlossenen Subsystemen oder sogar separat laufenden Applikationen benötigt. Diese werden gesammelt und bereitgestellt. Eine wesentliche Aufgabe ist es, an diese Information zu gelangen, diese in Zusammenhang zu bringen und bei entsprechender Anforderung dem kooperierenden Haus zur Verfügung stellen zu können.

Die Informationen werden ausschließlich bei Bedarf für die Übertragung bereitgestellt und sollen für die geplante Fortsetzung der begonnen Behandlung eingesetzt werden. Nach Möglichkeit soll eine automatische Zuordnung von Informationen zu bereits vorhanden Patientendaten in der anderen Empfängereinrichtung erfolgen. Bis zur Einführung der Gesundheitskarte mit einer eindeuti-

[2] s.a. Glossar

gen Versichertenidentifikation ist diese Anforderung über einen Master-Patient-Index (MPI[3]) zu realisieren.

Die Übertragung der Daten soll nur nach tatsächlichem Bedarf erfolgen, so dass die Übertragung von nicht benötigten Informationen vermieden wird. Dieses Vorgehen nach dem Minimalprinzip ist ebenfalls aus Sicht des Datenschutzes notwendig und sorgt gleichzeitig für eine Einsparung der Kommunikationskosten. „Nach außen angebotene Daten sollten auf das erforderliche Mindestmaß beschränkt werden“ (Helmbrecht 2004).

„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich danach an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen“ (Albert und Langerfeld 2004).

Für den Datentransfer ist eine geeignete und für weitere Anforderungen offene Infrastruktur zu konzipieren. Die Vorgaben aus dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik und der Einsatz zertifizierter Komponenten müssen unter Einbeziehung der Wirtschaftlichkeit berücksichtigt werden.

[3] s.a. Glossar

3 Abgrenzung

Das GMG befasst sich mit dem gesamten Gesundheitswesen in Deutschland und berücksichtigt dabei die Zusammenarbeit der einzelnen Bereiche bei der sektorübergreifenden Zusammenarbeit. Dabei sind neben den Krankenhäusern auch die niedergelassenen Ärzte, Einrichtungen der Rehabilitation und der Altenpflege, Apotheken etc. Teil des Ganzen.

Die vorliegende Arbeit fokussiert auf folgenden Aspekt des angestrebten Patientendatentransfers: sie behandelt die Kooperation zwischen Krankenhäusern, wobei ausdrücklich nicht ausgeschlossen wird, dass diese Architektur auch für die Kooperation anderer Bereiche sinnvoll und nutzbar ist. In diesem Zusammenhang sei auf die Zuweiserbindung verwiesen, bei der die Krankenhäuser durch die zeitnahe Bereitstellung von Informationen eines Krankenhausaufenthaltes eines Patienten dem einweisenden und weiterbehandelnden Arzt einen Mehrwert bieten und darüber hinaus mit weiteren Mitteilungen und Angeboten versorgen können.

Berücksichtigt wird jedoch vor allem, dass weitere Anforderungen auf diese Architektur zukommen und diese nach Möglichkeit in das Gesamtsystem integriert werden können wobei dies letztlich auf dem Hintergrund des „Return-of-Investement“ reflektiert wird.

Behandelt wird in dieser Arbeit kein konkreter Vertrag zur Integrierten Versorgung, der die genauen Modalitäten aus rechtlicher und monetärer Sicht festlegt und gegebenenfalls Arbeitsabläufe, die parallel zur elektronischen Kommunikation abgebildet werden müssen, definiert.

4 Das KIRP/V – Modell

Für eine strukturierte Betrachtung der Anforderungen, die entsprechend einen modularen Aufbau ermöglichen, habe ich zur Veranschaulichung das im Folgenden beschriebene KIRP/V - Modell entworfen, dessen Skizze als Diskussionshilfe dienen soll. Die Aufgliederung erfolgt dabei in 4 Ebenen, die einzelnen betrachtet werden können, was die notwendige Abstraktion der Ebenen zueinander ermöglicht. Auf der einen Seite wird so eine Betrachtung einzelner Aspekte vereinfacht, auf der anderen muss bei eventuellen Änderungen in der Anforderungsdefinition nicht das Gesamtkonzept neu überdacht und durch ein anderes ersetzt werden.

Die Grundidee resultiert aus der folgenden Überlegung, die mich veranlasst hat dieses Modell zu entwerfen, und für die erläuternde Diskussion zu nutzen:
Im Prinzip besteht die Problemstellung daraus, alle den Patienten betreffenden Informationen innerhalb eines Hauses in Zusammenhang zu bringen und ohne Medienbruch bearbeiten zu können. Ein Medienbruch liegt dann vor, wenn Informationen beispielsweise für eine Bearbeitung zunächst ausgedruckt werden muss und für die darauf folgende Informationsweiterleitung wieder digitalisiert werden muss. Diese Informationen zu gewinnen und die benötigte Integration zu gewährleisten ist entsprechend auch Aufgabe der Mitarbeiter innerhalb der Institution.

Wie der eigentliche Kommunikationsweg realisiert wird, ist aus für die höheren Schichten im Modell nicht relevant. Die Integration der Daten innerhalb eines Hauses und im Gegensatz dazu zwischen verschiedenen Institutionen des Gesundheitswesens setzt dabei lediglich eine sichere Kommunikation voraus. „Die Qualität der Kommunikation zwischen den Anbietern im Gesundheitswesen beeinflusst stark die Qualität der Heilbehandlung“ (van Bemmel und Musen 1997).

Die nachstehende Abbildung zeigt die 4 Ebenen

- Kommunikation (K),
- Integration (I),

- Repository (R) und
- Präsentation (P) sowie
- den Vertrag zur Integrierten Versorgung (V),

welche, mit Ausnahme des IGV[4]-Vertrages (Vertrag zur Integrierten Versorgung), in den nachstehenden Abschnitten ausführlich behandelt werden. Der Vertrag selbst würde ein eigenes Thema darstellen und weit über den Umfang dieser Arbeit hinausgehen. Er wird aber zunehmend eine Rolle spielen, wie die folgende Textstelle aufzeigt: „Unter dem Zwang der Kostendämpfung und den damit verbundenen Interventionsdrohungen des Gesetzgebers hat sich insbesondere zwischen Ärzten als Leistungserbringern und den Krankenkassen als Kostenträgern die Praxis durchgesetzt, so viel wie möglich unter den Vertragsparteien im Wege der Vereinbarung zu regeln“ (Buchholz 1988).

Mein Modell ist dezentral organisiert und besitzt daher keinen „Single Point of Failure“. Dadurch ist gewährleistet, dass das gesamte Netzwerk nicht zentral von einem Server aus verwaltet wird und somit zusammenbrechen könnte, falls dieser ausfällt oder gewartet werden muss. Außerdem bietet es daher mehreren Krankenhäusern die Möglichkeit in den Verbund aufgenommen zu werden.

[4] s.a. Glossar

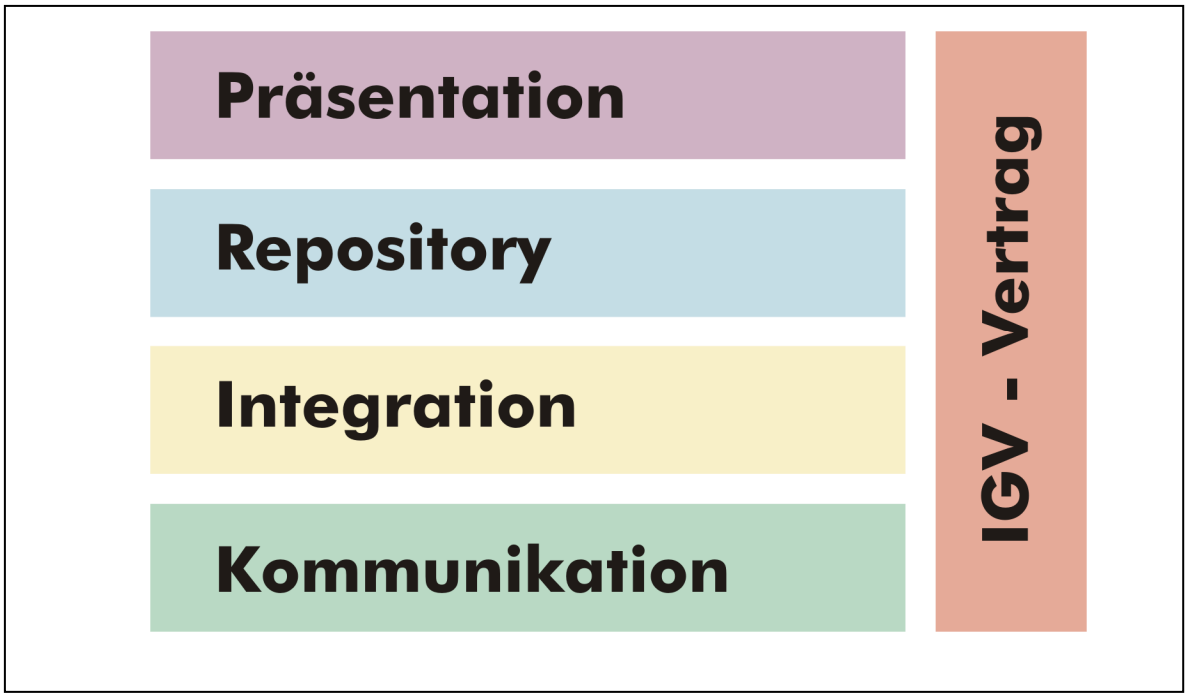


Abb. 1: KIRP/V Ebenen-Modell

4.1 Kommunikation

Wie bereits erwähnt ist der Kommunikationsebene im Zusammenhang mit den Anforderungen an einen hausübergreifenden Austausch von Patientendaten besondere Beachtung zu schenken. Genau an dieser Stelle existiert der größte Unterschied zur internen Kommunikation, und die Anforderungen an den Datenschutz bekommen höchstes Gewicht.

4.1.1 Anbindung

Die nachfolgenden Abschnitte befassen sich mit der Anbindung der jeweiligen Einrichtung, so dass eine Kommunikation überhaupt erst möglich wird. Im ersten Abschnitt wird eine allgemeine Sicht auf die physikalischen Aspekte behandelt. Darauf folgt die konkrete Argumentation, die für einen vom „normalen“ Internetzugang getrennten Übergang ins öffentliche Netzwerk plädiert.

Zunächst sollen die physikalische Anbindung diskutiert werden und, draus abgeleitet, die besonderen Anforderungen für die sichere Kommunikation. Technisch betrachtet existieren zahlreiche Möglichkeiten. Angefangen von einer echten, statischen Punkt-zu-Punkt Verbindung, realisiert als Digitale-Direkt-Verbindung (DDV[5]) eines Leitungsproviders über diverse dynamische Einwahlmöglichkeiten beim jeweiligen Kommunikationspartner bis hin zur DSL[6] Verbindung. Die einzelnen Möglichkeiten sollen hier nicht im Detail beschrieben werden. Aus den Erfahrungen zahlreicher Projekte und den speziellen Anforderungen scheint die Entscheidung für eine DSL-Verbindung aus wirtschaftlicher und technischer Sicht die erste Wahl. Der Vorteil dabei ist, dass diese ein sehr gutes Kosten- und Nutzenverhältnis aufweist und in der Regel schnell verfügbar ist. Dazu kommt das breite Spektrum der angebotenen Bandbreiten, die je nach Datenvolumen unterschiedlich hoch sein können. In der konkreten Architektur werden Informationen zunächst der empfangenden Einrichtung zur Verfügung gestellt. Nach Abschluss der Behandlung werden die Informationen vom HDZ

[5] s.a. Glossar
[6] s.a. Glossar

für das überweisende Haus bereitgestellt. Davon ausgehend ist der Betrieb einer SDSL[7]-Anbindung sinnvoll, bei der gegenüber einer ADSL-Leitung beide Datenrichtungen über die gleiche Bandbreite verfügen, z.B. 1 MBit/s. Hierbei wäre gewährleistet, dass Daten genauso schnell gesendet, wie empfangen werden können. Eine fest zugeordnete IP-Adresse[8] wird benötigt und stellt bereits den ersten Schritt in Richtung Sicherheitslösung dar.

Den Vorteilen stehen jedoch auch zwei Aspekte gegenüber, die gesondert betrachtet werden müssen. Beide beruhen auf der Tatsache, dass der Datentransfer über das öffentliche Internet erfolgt und somit zunächst nicht für die Übertragung besonders schützenswerter Informationen geeignet ist. Dies hat zur Folge, dass es im Gegensatz zu einem geschlossenen Netz zu einem hohen Datenaufkommen durch andere Teilnehmer des Netzes kommen kann und keine Garantie über einen Mindestdurchsatz gegeben werden kann. Die vorliegenden Anforderungen erwarten zwar eine zeitnahe Abwicklung des Informationsaustausches, jedoch keine Übermittlung in Echtzeit. Die Erfahrungen der letzten Jahre zeigen aber, dass eine solche Anbindung den Anforderungen genügt.

Bei Anbindungen mittels DSL oder Einwahl wird häufig der Einsatz einer dynamischen IP-Adresse präferiert. Problematisch ist dabei, dass die meisten Provider nach einer fixen Zeitspanne, meist 24 Stunden, die Verbindung „künstlich“ trennen, so dass die entsprechenden Router sich erneut anmelden müssen. Bei dieser Konnektierung wird ihnen eine neue, freie IP-Adresse zugeordnet. Dies ist in soweit nachteilig, als dass es bei Nutzung von verfügbaren, größtenteils kostenlosen Diensten für die Namensauflösung von dynamischen IP-Adressen[9] (beispielsweise dyndns.org) zu Zeitverzögerungen kommen kann. Sind die Ser-

[7] s.a. Glossar

[8] Die statische IP-Adresse identifiziert den Netzanschluss im Internet eindeutig und lässt sich so von extern problemlos über die Adresse direkt oder über einen zugeordneten Namen, der über die Domain Name Server (DNS) publiziert wird, ansprechen.

[9] Die dynamische IP-Adresse wird bei der Verbindung zum Provider zugewiesen. In der Regel erhält der Benutzer durch ein erneutes konnektieren eine andere IP-Adresse aus dem Pool des Providers. Eine eindeutige Identifizierung ist damit nicht möglich.

ver des Dienstanbieters nicht verfügbar, so wird auch der Name nicht mehr einer IP-Adresse zugeordnet werden können. Ein weiteres Manko ist, dass viele Anbieter von VPN[10]-Lösungen Probleme bei dem Aufbau einer VPN-Verbindung haben, wenn beide Knoten mit dynamischen Adressen agieren.

Die Parameter der benötigten Anbindung hängen vom Datenvolumen, vom benötigten Durchsatz und deren Richtung ab. Werden hauptsächlich Daten empfangen und nur wenige versendet, so kann der Einsatz einer günstigen ADSL-Leitung ausreichen. In der Regel wird jedoch auch der Datenstrom nach extern gewissen Anforderungen entsprechen müssen. Entscheidend ist dann weiter die Bandbreite. Für eine asynchrone Kommunikation oder einen Datenaustausch, der keinen zeitkritischen Anforderungen unterliegt, kann eine kleinere Bandbreite ausreichend sein. Für Wartungszwecke mit dem Bedürfnis einer entsprechenden Performanz sind die Erfordernisse höher.

In fast allen Häusern existiert bereits ein zentraler Zugang in das öffentliche Internet, der den Mitarbeitern der Einrichtung entsprechende Dienste zur Verfügung stellt. In einigen Fällen existieren sogar zwei voneinander getrennte Netze, so dass das produktive LAN[11], in denen das KIS betrieben wird, keine Verbindung zum Internet hat. Ein speziell dafür eingerichtetes Netzsegment oder sogar physikalisch entkoppeltes Netzwerk wird dann für diese Dienste eingerichtet.

Hinsichtlich der Anforderung, dass Daten aus dem KIS externen Kommunikationspartnern zur Verfügung gestellt werden sollen, würde man aber auch bei einem separaten Netzwerk nicht umhin kommen, das produktive Netz mit dem Internet zu verbinden, und zwar unter Berücksichtigung der noch im Detail zu besprechenden Sicherheitskriterien.

Eine in diesem Zusammenhang häufig getroffene und zunächst nachvollziehbare Aussage präsentiert den Vorschlag, den bestehenden Internetzugang eben-

[10] s.a. Glossar
[11] s.a. Glossar

falls für den Datenaustausch zu nutzen. Dafür sprechen sicherlich die bereits getätigten Investitionen in die Absicherung des Netzwerkes durch Komponenten, die später noch im Einzelnen behandelt werden. Hinzu kommen die Leitungskosten, die monatlich ein vereinbartes festes (Flatrate[12]) oder nach Nutzung definiertes Volumen beinhalten.

Den zusätzlichen Kosten für die Anschaffung der benötigten Komponenten sowie dem erhöhten administrativen Aufwand durch die Pflege von zwei Übergängen in das Netzwerk steht als Vorteil die signifikante Erhöhung der Datensicherheit gegenüber.

Auch wenn der Zugang für Mitarbeiter in das Internet für E-Mail, Informationsrecherche und weitere Dienste überwacht und durch zusätzliche Sicherheitseinrichtungen gesteuert wird, sollte für den Austausch von Patientendaten immer eine separate Anbindung gewählt werden.

Dafür spricht, dass in einer solchen Konfiguration tatsächlich nur die Dienste erlaubt werden, die für den Datenfluss benötigt werden. Da die kommunizierenden Partner in aller Regel bekannt sind und Dritte ohne Einwilligung keinen Zugang bekommen, kann ein sehr fein granuliertes Sicherheitssystem eingerichtet und verwaltet werden. Die Überwachung an diesem Knoten betrifft dann tatsächlich nur die sicherheitsrelevanten Daten. Die zusätzliche Anbindung kann heute kostengünstig realisiert werden.

[12] s.a. Glossar

4.1.2 Sicherheitskomponenten

Die Ansprüche an die Sicherheit werden durch den Einsatz entsprechender Komponenten erfüllt. Alleine die Nutzung erprobter und zertifizierter Geräte reicht jedoch nicht aus, um eine sichere Kommunikationsplattform zu realisieren und zu betreiben. Wesentlicher Ausgangspunkt ist das zugrunde liegende Konzept, welches sämtliche Gesichtspunkte in Augenschein nimmt.

Die nachfolgenden Abschnitte beschreiben zunächst wesentliche Funktionalitäten, Komponenten und Begrifflichkeiten, wie sie in einem Sicherheitsszenario berücksichtig werden müssen. Diese werden erst vorgestellt, so dass anschließend die Architektur nachvollzogen werden kann.

Zunächst ist die Firewall[13]-Funktionalität die entscheidende Komponente für den Aufbau der benötigten Infrastruktur. Allgemein besteht eine Firewall aus einer oder mehreren Hard- und Softwarekomponenten, die zwei Netzwerke koppeln und sicherstellen, dass jeglicher Verkehr dazwischen durch die Firewall geleitet und überprüft wird. Sie realisiert eine Sicherheitsstrategie, die Zugriffsrestriktionen und gegebenenfalls Protokollierungs- und Authentifikationsanforderungen umfasst. Eine Firewall leitet nur diejenigen Datenpakete weiter, die diese Anforderungen erfüllen.

Zu beachten ist, dass eine Firewall aber keineswegs den Einsatz weiterer Sicherheitsmaßnahmen und –mechanismen erübrigt, sondern lediglich ein wesentlicher Baustein der IT-Sicherheit ist. Zu beachten ist weiterhin, dass Firewalls keinen Schutz vor internen Angriffen bieten. Unerlaubte Zugriffe durch andere Netzzugänge (Modems, ISDN etc.) sind prinzipiell weiter möglich und bieten nur geringfügigen Schutz vor datengetriebenen Angriffen, z.B. durch virenverseuchte Programme und Daten sowie bösartige JAVA-Applets[14].

[13] s.a. Glossar
[14] s.a. Glossar

Die Anforderungen an eine moderne Firewall gehen über die einfache Konfiguration des Regelwerks hinaus. Sie berücksichtigen ebenfalls alle weiteren Schwachpunkte, die einem Angreifer einen Zugriff auf das Netz bzw. auf das Firewallsystem an sich ermöglichen könnte. So ist ein wesentlicher Faktor die Trennung von der eigentlichen Firewall-Funktionalität und dem Management sowie dem Log-Server.

Sämtliche Konfigurationen sollten durch den Zugriff auf die Managementkonsole ausgeführt werden können, so dass auf die eigentlichen Firewall-/VPN-Knoten kein Zugriff erforderlich ist. Dabei ist zu berücksichtigen, dass die Verbindung zum Managementsystem ebenfalls durch Verschlüsselung und Authentifikation gesichert ist. Das Regelwerk sollte zweistufig modifiziert werden können, so bleibt dem Administrator die Möglichkeit die Änderungen in Summe zu überprüfen, bevor diese auf dem Echtsystem wirksam werden.

Abhängig von der Administration der Firewall, zum Beispiel entweder durch einen Mitarbeiter im Haus oder ein externes Dienstleistungsunternehmen, sind oftmals verschiedene Administrations-Level sinnvoll. Die Zugriffe zu Modifikationen auf das Regelwerk sollten dabei nach Möglichkeit durch das System protokolliert werden.

Bei der Verwaltung mehrer Firewalls, z.B. in verteilten Umgebungen, redundanten Systemen oder beim Aufbau einer demilitarisierten Zone (DMZ[15]), ist ein zentrales Management essentiell. Ein weiterer wichtiger Aspekt sind die Anforderungen an das Logging. Für die Auswertungen sollten bereits vom System Reporting-Tools im Lieferumfang enthalten sein.

Die Art und Weise wie Informationen ablegt und bearbeitet bzw. ausgewertet werden können, sind ebenfalls wichtiger Bestandteil einer Firewall-Pflege. So wird es einem Administrator überhaupt erst ermöglicht, zeitnah und effektiv bei eventuellen Angriffen zu reagieren. Dazu gehört selbstverständlich auch die

[15] s.a. Glossar

Alarmfunktionalität, die auf Verstöße gegen die vereinbarte Policy aufmerksam macht. Grundsätzlich sollte das System natürlich die Funktionalitäten „packet filtering“, „stateful inspection“ und „application-level security“ unterstützen.

Für die Pflege der Firewall bezüglich Updates und Patches ist die Verfahrensweise von Interesse, die je nach Konstellation zu Problemen oder Unsicherheiten führen kann. Von Vorteil ist dabei, wenn die Firewall ihr eigenes Betriebssystem mitbringt, so dass es an dieser Stelle nicht zu Inkompatibilitäten kommen kann und die Ausfallszeit bei Problemen so gering wie möglich bleibt.

Der Konfiguration einer Firewall sollte eine Erstellung eines Regelwerkkatalogs vorweg gehen. Dieser stellt gleichermaßen eine Art Lastenheft für die Konfiguration der Sicherheitskomponenten dar und kann in der Folge als Basis einer Dokumentation dienen. Prinzipiell ist nach dem Minimal-Prinzip vorzugehen, bei dem zunächst sämtlicher Verkehr für alle unterstützten Protokolle verboten wird. Entsprechend der Anforderungen und Bedürfnisse einzelner Applikationen werden die notwendigen IP-Adressen und die zugehörigen Ports frei geschaltet. Unter Umständen sind an dieser Stelle auch Maßnahmen wie Port Address Translation (PAT) bzw. Network Address Translation (NAT) notwendig, so dass beispielsweise über eine einzige IP-Adresse verschiedene Applikationen auf diversen Servern angesprochen werden können.

Nach der Festschreibung der Konfiguration ist diese im nächsten Schritt auf ihre Integrität und Anforderungskonformität zu überprüfen. Die letzte Maßnahme ist, durch entsprechende Tests an den betroffenen Komponenten, die Wirksamkeit der umgesetzten Policies zu überprüfen. Die zweite und dritte Phase sollten nach umfangreicheren Modifikationen am Regelwerk selbstverständlich erneut durchgeführt und deren erfolgreiche Erledigung protokolliert werden.

Nach der Installation und Konfiguration der Firewall folgt der laufende Betrieb des Sicherheitssystems. Bis zu einem gewissen Grad ist an den entsprechenden Komponenten keine weitere Modifikation mehr notwendig. Ausgenommen davon sind sicherlich die regelmäßigen Watungsarbeiten, die auch im Zusammenhang mit der Schwachstellenanalyse angesprochen werden.

Dennoch ist es notwendig, die Log-Dateien in fixen Zeitabständen zu bearbeiten. Dabei ist die Konfiguration der Granularität der protokollierten Daten wesentlich entscheidend für eine möglichst effektive Administration der Firewall.

Bei der späteren Auswahl der Produkte ist ebenfalls der Qualität des Reportings eine große Gewichtung zuzuordnen. Überwiegend unterscheiden sich die Systeme der führenden Anbieter nicht in ihrer Qualität bei der Umsetzung der konfigurierten Regeln, wohl aber bei der Art und Weise der Konfiguration, die beliebig kompliziert ausfallen kann. Viel wichtiger für den laufenden Betrieb ist neben Optionen zum Logging und den vordefinierten Reports und Statistiken die Möglichkeit, eigene Auswertungen zu definieren, um regelmäßig und übersichtlich über potenzielle Angriffsversuche informiert zu sein.

Die „demilitarisierte Zone“ (DMZ[16]) stellt einen speziellen Bereich innerhalb eines Computernetzes dar. Es handelt es sich dabei um einen geschützten Rechnerverbund, der sich zwischen 2 Netzwerken befindet.

Denkbare Szenarien sind die beiden folgenden:

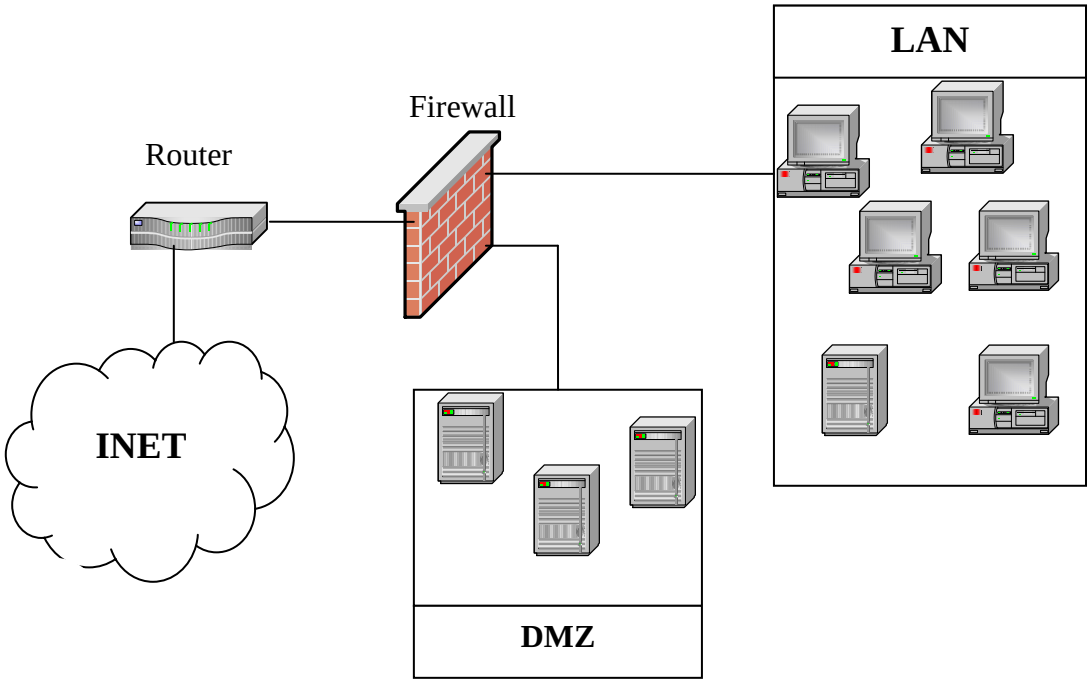


Abb. 2: DMZ Szenario A

[16] s.a. Glossar

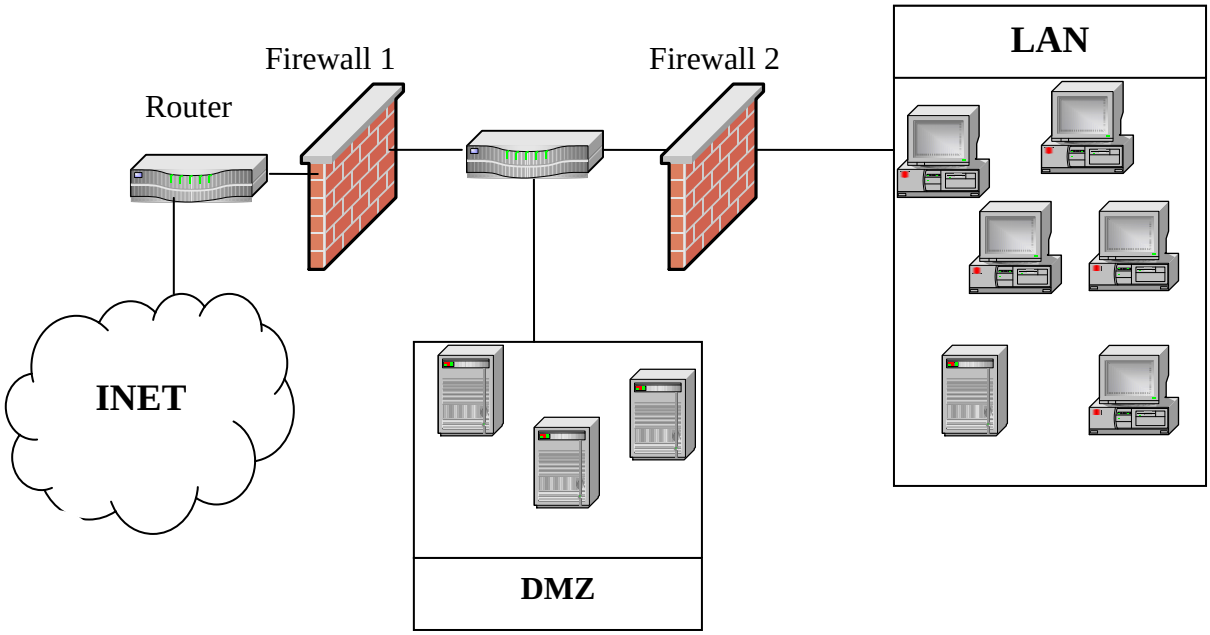


Abb. 3: DMZ Szenario B

Der Sinn des Aufwandes ist es, möglichst auf sicherer Basis Dienste des Rechnerverbundes (z.B. E-Mail oder Datenbanken) sowohl dem einen als auch dem anderen Netz zur Verfügung zu stellen.

Die in Szenario B beschriebene Variante birgt den Vorteil, dass die beiden Firewall-Knoten getrennt voneinander konfiguriert werden können. Aus sicherheitstechnischen Gründen werden in großen Netzwerken die jeweiligen Firewalls redundant angelegt. Auch nach Veröffentlichungen des Bundesamt für Sicherheit in der Informationstechnik (BSI): „… empfiehlt sich ein mehrstufiges Firewallkonzept, bei dem zusätzliche Filterelemente (beispielsweise Router) vor- und nachgeschaltet werden“ (Helmbrecht 2004).

„…Eine Firewall sollte mindestens aus zwei hintereinander angeordneten Systemen bestehen, um auch bei Ausfall einer Komponente (z. B. durch einen Programmierfehler oder einen Konfigurationsfehler) ein Überwinden der Firewall zu verhindern“ (BSII 2003) und „…bei hohem Schutzbedarf ist ein 2-stufiges Fire-

wallsystem … die minimale Anforderung an eine Internet-Anbindung“ (Veit 2000).

Aus Kostengründen und Aspekten der Wartung bzw. des Managements des Firewallsystems sollten namhafte Hersteller gewählt werden, bei denen die Qualität durch zeitnahe Aktualisierung ihrer Systeme auch nach Auftreten von sicherheitsrelevanten Schwachstellen hoch ist.

Wie bereits zum Thema Logging und Reporting angesprochen, ist es normalerweise nicht ausreichend ein einmal in Betrieb genommenes Firewallsystem mit seinen statischen Regeln ohne weitere Administration zu betreiben. Neben der regelmäßigen Auswertung von Log-Dateien ist in periodischen Abständen die Sicherheitsqualität der Sicherheitskomponenten zu überprüfen und zu aktualisieren. Immer wieder melden auch führende Softwarehersteller von Security-Systemen, dass eine Sicherheitslücke in deren Applikationen entdeckt wurde und stellen entsprechende Patches zur Verfügung. Diese sind nach Möglichkeit zeitnah einzupflegen, da auch die „andere Seite“ über diese Informationen verfügt und versucht diese Informationen zu nutzen, um in solche Systeme einzudringen bzw. im Sinne von „Denial of Service“ – Attacken deren Betrieb zu stören.

Neben diesem manuellen Verfahren, also Newsletter zu abonnieren und regelmäßig die einschlägigen Seiten der Hersteller und Nutzergruppen zu lesen, existieren auch Werkzeuge, die mittels aktueller Informationen auf mögliche Schwachstellen prüfen und entsprechende Auswertungen zur Verfügung stellen.

Wesentlicher Bestandteil der sicheren Kommunikationsinfrastruktur neben der Firewall ist die Funktionalität der „Virtuellen Private Netzwerke“ (VPN). Durch die Zusammenhänge in der Konfiguration von Firewall- und VPN-Regeln ist in den meisten Fällen eine integrierte Lösung sinnvoll. Die meisten Firewall-Hersteller bieten diesen Dienst bereits als integralen Bestandteil ihrer Lösung an oder aber als Option. Vorteilhaft ist dabei außerdem, dass die selben Werkzeuge zur Verfügung stehen und die Konfiguration über dieselbe Oberfläche zu tätigen ist, wie es für die Verwaltung des Firewall-Systems geschieht.

Die Arbeitsweise eines Virtuellen Privaten Netzes setzt sich aus zwei grundsätzlichen Bestandteilen zusammen. Auf der einen Seite wird eine Punkt-zu-Punkt-Verbindung zwischen zwei Kommunikationspartnern hergestellt, die den Netzwerkzugriff transparent macht. Für den externen Kommunikationspartner geschieht der Zugriff, ohne dass er berücksichtigen muss, dass der Datenverkehr über ein fremdes Netz geleitet wird. Er greift auf Ressourcen im entfernten Netz zu, als ob es sich um lokale Betriebsmittel handeln würde. Auf der anderen Seite wird diese Verbindung verschlüsselt.

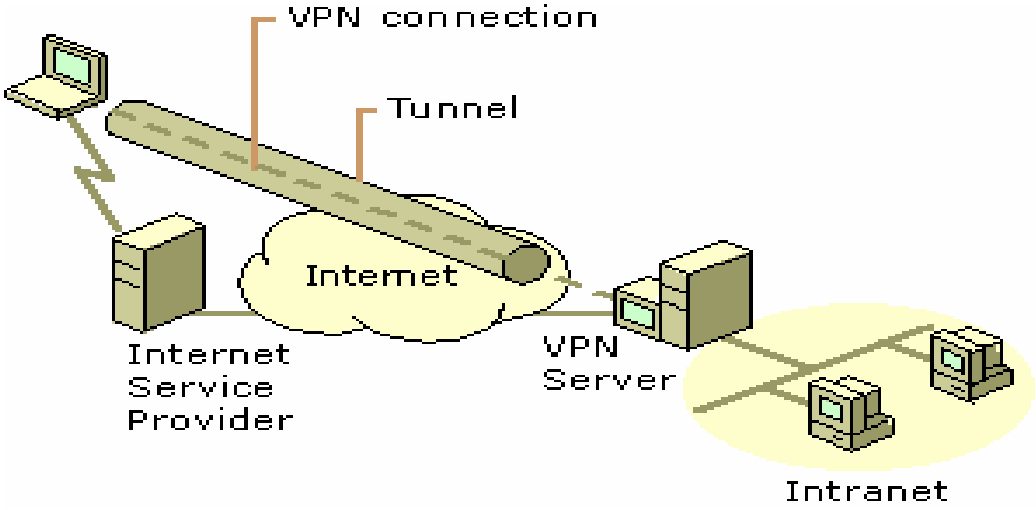


Abb. 4: VPN

Bei der Auswahl von Anbietern für VPN-Lösungen ist darauf zu achten, dass eine möglichst weit reichende Kompatibilität zu anderen Herstellern nachweislich vorhanden ist und nicht nur die Produkte eines Herstellers problemlos miteinander die gewünschten sicheren Kanäle aufbauen können. Der Nachweis einer solchen Kompatibilität wird von verschiedenen Testcentern erbracht. Eine der bekannteren Informationsquellen ist über die Web-Site http://www.vpnc.org zu erreichen. Das Konsortium, welches sich dahinter verbirgt, hat es sich zur Aufgabe gemacht, die Kompatibilität der Produkte diverser Hersteller zu erhöhen und Hilfestellung bei Einführung und Betrieb von VPN-Konfigurationen zu geben. Getestet werden alle namhaften Hersteller, welche wiederum Informationen für eine interoperable Implementierung zur Verfügung stellen.

Bei der Auswahl eines Anbieters sind der Umgang mit Verschlüsselungstechniken, den eingesetzten Hash-Verfahren und der Austausch von Schlüsseln bzw. Zertifikaten von Interesse. Außerdem kommt den eingesetzten Authentifizierungsverfahren eine bedeutende Beachtung zu. Vor allem in heterogenen Netzen, in denen vorhandene Komponenten integriert werden müssen, oder wenn dem Kommunikationspartner kein Produkt vorgeschrieben werden kann, ist auf diese Aspekte zu achten. Dadurch wird eine möglichst hohe Kompatibilität gewährleistet.

Unterschieden werden kann zwischen einer „Client–Gateway“- und einer“ Gateway-Gateway“-Verbindung. Sinnvoll bei beiden Varianten ist der Einsatz eines symmetrischen Verschlüsselungsalgorithmus. Der Vorteil asymmetrischer Kryptographien liegt im einfachen Verbindungsaufbau, welchen die Nutzung von privaten und öffentlichen Schlüsseln zu Grunde liegt. Symmetrische Kryptosysteme, wie beispielsweise 3DES, haben dagegen eine gute Performance hinsichtlich der Verschlüsselungsgeschwindigkeit und Implementierung in Hard- und Software-Umgebungen. Die Sicherheit, die symmetrische Verfahren bieten, ist ausreichend, wenn Schlüssel mit einer Länge von 128 Bits und mehr verwendet werden. Der Hauptnachteil ist die sichere Verteilung der Schlüssel.

„Asymmetrische Verschlüsselungssysteme werden also in der Praxis wegen des sehr hohen Rechenbedarfs lediglich zur Verschlüsselung von sog. „Sitzungsschlüsseln“ (Session Keys) verwendet. Die Verschlüsselung der eigentlichen Nutzdaten findet dann mit einem klassischen symmetrischen Verfahren unter Verwendung des jeweiligen Sitzungsschlüssels statt. In diesem Falle spricht man von einer hybriden Chiffrierung (asymmetrisch / symmetrisch)“ (Goetz und Sembritzki 1998).

Die Gateway-Gateway-Kommunikation kann durch den Austausch standardisierter Zertifikate auf Basis des X.509-Protokolls erfolgen. Die Client-Authentifizierung sollte zusätzlich über Verfahren wie Radius oder LDAP erfolgen können bzw. token-basierte Verfahren berücksichtigen.

Im Hinblick auf die Zugriffe auf das interne Netzwerk ist für diese Verbindungen, die letztlich keiner Einschränkung mehr unterliegen, der Einsatz einer besitzbasierenden Authentifizierung zu empfehlen, welche gewährleistet, dass diese Benutzerprofile durch keinerlei Attacken auf die Entschlüsselung von Kennwörtern (beispielsweise „Brute Force“) durch unautorisierte Dritte genutzt werden können.

Vor allem bei der Firewall als wichtigster Baustein einer IT-Sicherheitsinfrastruktur steht die Frage nach vorhandenen Zertifizierungen nicht an letzter Stelle. Dabei ist es prinzipiell möglich nach den Vorschlägen des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorzugehen. Das BSI testet und zertifiziert allerdings in der Regel lediglich nationale Produkte. Entsprechend existieren internationale Prüfgremien wie beispielsweise CC (Common Criteria) und ITSEC (International Trusted Computer System Evaluation Criteria). Für die Anerkennung der Common Criteria hat die Bundesrepublik Deutschland sowie eine große Anzahl weiterer europäischer Länder einen Ver-

trag geschlossen. Bei dieser Zertifizierung existieren so genannte „Evaluation Assurance Level“ (EAL), die den einzelnen Produkten vergeben werden.

Bei der Auswahl eines Firewall-Systems sowie der VPN-Funktionalität sollte auf ein solches Gütesiegel geachtet werden.

4.1.3 Die Patientendaten-Transfer-Zone (PDTZ)

Aus den bekannten und oben geschilderten Erkenntnissen kann nun die entsprechende Architektur als sichere Kommunikationsplattform abgeleitet werden. Dabei gilt es die entscheidende Forderung an den Datenaustausch zu berücksichtigen. Es sollen den Kommunikationspartnern besonders schützenswerte Daten zwar zur Verfügung gestellt werden, dennoch ist der Aufbau jeglicher Kommunikationskanäle in das produktive LAN zu unterbinden. Als Ausnahmen in diesem Zusammenhang könnten spezielle Wartungszugänge für die Mitarbeiter des Hauses angedacht werden, die jedoch nach den obigen Ausführungen zur Authentifizierung, abzusichern sind.

Für sämtlichen Datentransfer sollte immer der Gedanke einer Schleuse verfolgt werden. Eingehende Informationen treffen zunächst in einer DMZ[17] ein, werden zwischengespeichert und von dort weitergeleitet. Je nach Protokoll und Datenart kann an dieser Stelle eine Viruswall[18] den Datenstrom auf Viren, Bakterien, Trojaner und Würmer untersuchen oder sonstige unerwünscht Daten (SPAM) fernhalten. Nun würde die DMZ von der Idee her die Anforderung erfüllen, keine direkte Verbindung ins LAN zuzulassen, egal, ob an einem weiteren Netzwerkdevice der ersten Firewall oder als Zone zwischen den beiden Firewalls realisiert.

Jedoch steht die nachvollziehbare Forderung im Raum, nach der in der DMZ keine Patientendaten permanent gespeichert werden dürfen. Für einen dateiba-

[17] s.a. Glossar
[18] s.a. Glossar

sierten Austausch könnte dies bereits problematisch sein, denn es ist nicht definiert, wie groß der Zeitraum zwischen Einstellen der Daten und Abholung durch interne Systeme sein darf.

Um größtmögliche Sicherheit zu erreichen und die wichtigen Daten kontrolliert zur Verfügung stellen zu können, wird meiner Einschätzung nach ein zusätzlich gesicherter Bereich benötigt. Dieser kann weder als DMZ bezeichnet werden, noch ist er dem produktiven LAN zugehörig.

Wie in Hinblick der erweiterten Anforderungen auf den sicheren Datenaustausch im Rahmen der Integrierten Versorgung deutlich wurde, ist der Aufbau einer entsprechenden Infrastruktur eine wesentliche Voraussetzung, um den datenschutzrechtlichen Anforderungen Rechnung zu tragen.

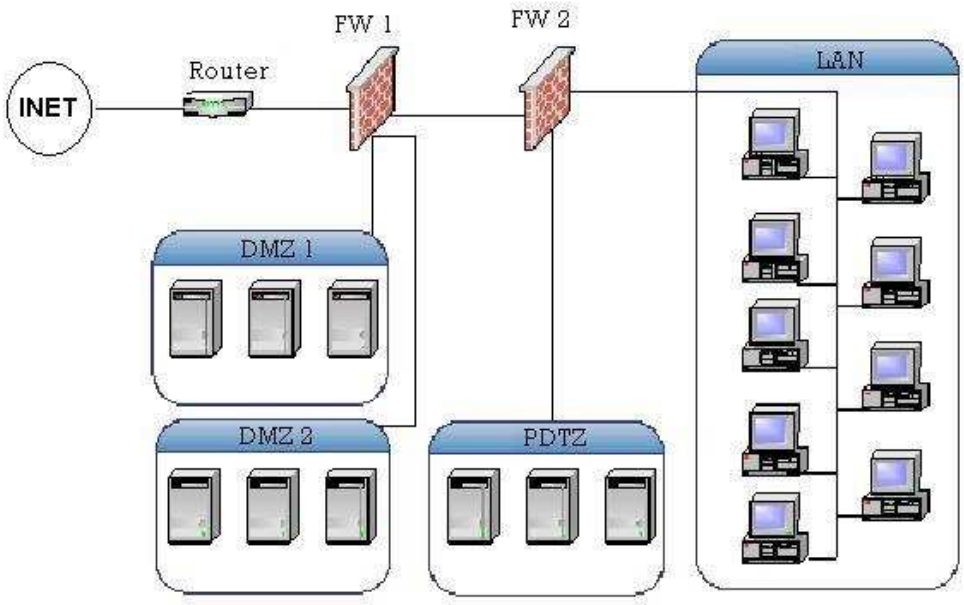
Aus diesen speziellen Betrachtung und den erhöhten Sicherheitsanforderungen heraus habe ich den Begriff Patientendaten-Transfer-Zone (PDTZ[19]) bei der konzeptuellen Betrachtung der Sicherheitsstrategie im Gesundheitswesen kreiert. Die PDTZ gewährleistet neben der demilitarisierten Zone (DMZ) als weitere Ebene den sicheren Datenaustausch. Diese Begrifflichkeit erleichtert die Kommunikation in einem Projekt in hohem Maße, da die dadurch bezeichnete Sicherheitszone sofort begriffen wird und in der Diskussion die gewünschte Assoziation darstellt.

Von außen betrachtet, wird sie an der zweiten Firewall konfiguriert und beherbergt dort die für die Übertragung von bereitgestellten Patienteninformationen. Vom Prinzip her könnte man diesen Bereich als DMZ-2 bezeichnen, was aber in der Diskussion wieder missverständlich sein würde, da ja auch mehrere unterschiedliche DMZ an der ersten Firewall installiert werden können. Parallel dazu könnte man die Position einnehmen, dass dieser besondere Bereich der PDTZ der Idee eines segmentierten Netzwerks nachkommt und somit neben dem produktiven LAN als LAN-2 bezeichnet werden könnte.

[19] s.a. Glossar

Dieser Bereich der PDTZ stellt prinzipiell keine zusätzlichen Anforderungen an die eingesetzten Sicherheitskomponenten, sondern entspricht parallel zur DMZ lediglich einer entsprechenden Konfiguration, welche allerdings eine signifikante Steigerung der Datensicherheit hervorbringt.

Die Bezeichnung PDTZ und das speziell darauf ausgerichtete Regelwerk ist eine logische Konsequenz aus den missverständlichen Begrifflichkeiten bei der Diskussion um den Aufbau einer Sicherheitsarchitektur in der Integrierten Versorgung.



Legende	
INET	Internet
FW	Firewall
DMZ	Demilitarisierte Zone
LAN	Local Area Network
PDTZ	Patienten Daten Transfer Zone

Abb. 5 Patientendaten-Transfer-Zone (PDTZ)

Bereits jetzt zeigt sich in Diskussionen der Vorteil eines eigens verwendeten Begriff für diese spezielle Zone, der Patientendaten-Transfer-Zone.

4.2 Integration

Die nächste Ebene, im KIRP/V-Modell oberhalb der Kommunikation angeordnet, betrifft die Thematik der Integration.

Das Ärzteblatt berichtet, dass „Die Gründe für die zahlreichen Informations- und Kommunikationsbrüche … unter anderem in der Verschiedenartigkeit und mangelnden Integration der vorhandene Datenformate und IT-Systeme sowie in fehlenden Standards und Normen [liegen]“ (Krüger-Brand 2003).

Die derzeitige Situation und die Anforderungen hinsichtlich der vorliegenden Spezifikation zeigen den wachsenden Bedarf der Optimierung wirtschaftlicher Vorgänge unter Zuhilfenahme von Informationstechnologien, welche zunehmend eine Schlüsselrolle im Gesundheitswesen einnimmt. Durch die starken Veränderungen kommt es zu einer zunehmenden Spezialisierung von Anbietern und dem Einsatz von komplexen Spezialsystemen, die umständlich in die bestehende Systemlandschaft integriert werden müssen. Dieser Bedarf wird deutlich, betrachtet man die Abläufe und die Tatsache, dass alle Informationen an ihrem Entstehungsort erfasst werden sollen, und dies nur einmal. Diese Informationen sind allen anderen Anwendungssystemen zur Verfügung zu stellen, um eine ganzheitliche Sicht auf den Informationsbedarf zu erhalten.

Durch die veränderte Interessenlage, nicht unbedingt alle Systeme eines Herstellers zu nutzen, sondern vielmehr jeweils für die diversen Funktionsbereiche die beste Auswahl zu treffen, kommt es zu einer vergleichbar hohen Heterogenität in der Systemlandschaft eines Krankenhauses.

Betrachtet man die zunehmende Zahl der eingesetzten Anwendungssysteme, die miteinander kommunizieren müssen, um strukturiert Daten auszutauschen, wird schnell deutlich, dass dies nicht durch den Einsatz proprietärer Schnittstellen von jeweils jedem zu jedem anderen System mit dann in Summe n:n-Beziehungen möglich ist.

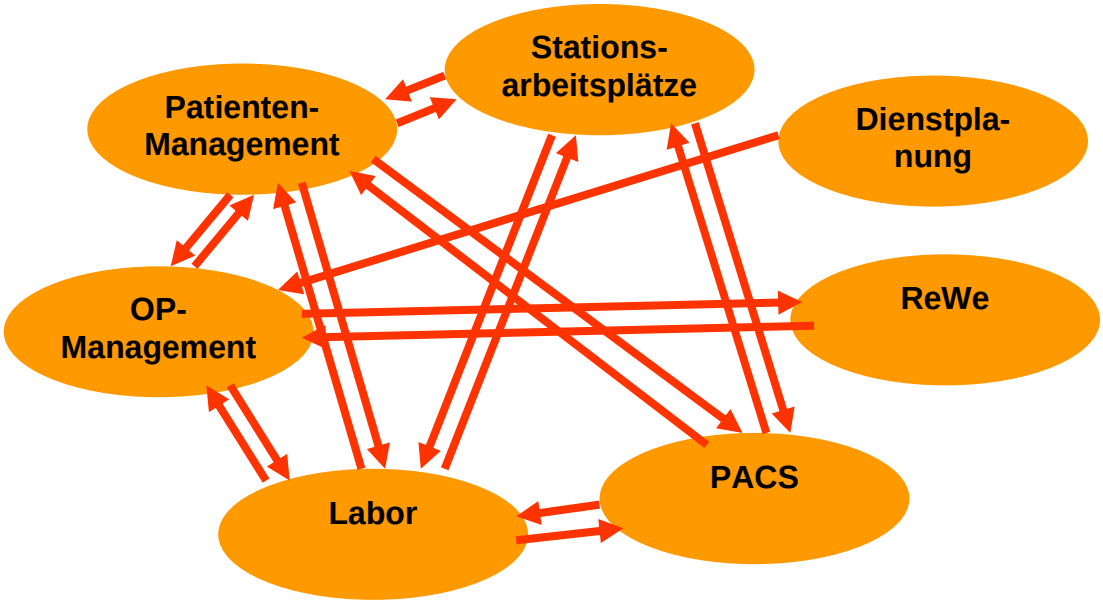


Abb. 6: Kommunikation ohne Integrationsserver

Im ursprünglichem Fall existieren n*(n-1) Verbindungen, die administriert werden müssen und bei Austausch eines Systems zu einem enormen Kostenfaktor werden können. Das Management einer solchen Struktur ist denkbar aufwändig und kann im Fehlerfall nicht zumutbare Ausfallzeiten nach sich ziehen.

Die Reduzierung der vorangestellten Schilderung der Schnittstellenkomplexität, wird durch Einsatz eines Integrationsservers[20] ermöglicht. Dieser, oft auch Schnittstellenserver genannt, dient als Datendrehscheibe mit zentralem Schnittstellenmanagement. An dieser Stelle soll der Begriff Integrationsserver explizit vom häufig benutzen Begriff des Kommunikationsservers[21] unterschieden werden. Ein Kommunikationsserver entspricht einer Plattform, die den Austausch von Daten in einer höheren Ebene bezeichnet und konkret Dienste wie E-Mail, das Surfen im Internet, „Voice-over-IP“, Faxdienste und so weiter umfasst. Der Integrationsserver in seiner Eigenschaft erfüllt die Anforderung nach Datenaustausch zwischen Systemen und stellt die benötigten Dienste und Protokolle zur

[20] s.a. Glossar
[21] s.a. Glossar

Verfügung, so dass der Austausch von verschiedenen Datenformaten von und zu unterschiedlichsten Datenquellen erfolgen kann.

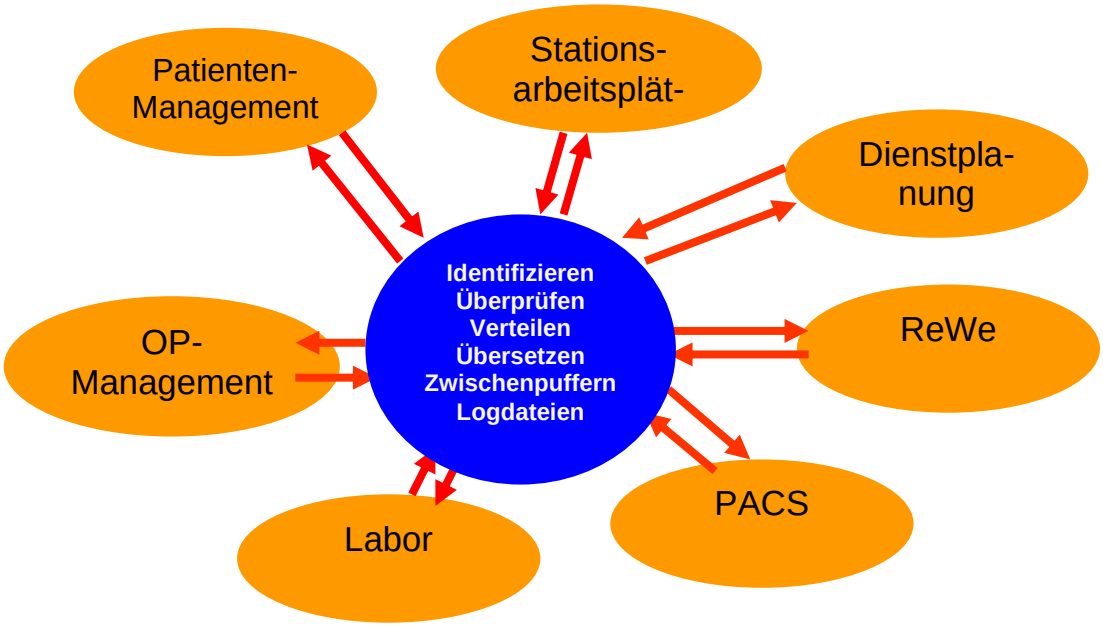


Abb. 7: Kommunikation mit Integrationsserver

Die Vorteile bei Einsatz eines solchen Servers sind einleuchtend, betrachtet man die verfügbaren Systeme am Markt. Immer wiederkehrende Anforderungen an den Datenaustausch müssen nicht neu entwickelt werden, sondern können sich einer bewährten Technik bedienen. Ein Integrationsserver ist in der Lage, simultan beliebige Nachrichtenformate, wie zum Beispiel HL7, DICOM, XML, ADT, LDT sowie proprietäre Strukturen, zu verarbeiten und erledigt dies auf unterschiedlichsten Protokollen von X.400 bis hin zu TCP/IP.

Der Austausch der Daten kann socket-basiert, als Filetransfer oder über andere Methoden wie RFC, ODBC etc. erfolgen.

Aktuelle Integrationsserver verfügen dabei über eine große Bibliothek für den kostengünstigen Anschluss und die Verwaltung der Schnittstellen beinahe aller eingesetzten Systeme im Gesundheitswesen.

Der Integrationsserver ist für das Zusammentragen, Umwandeln und zur Verfügung Stellen der notwendigen Informationen innerhalb des produktiven Netzwerks zwingend erforderlich. Aus den Diskussionen um die sichere Kommunikation wird deutlich, dass kein direkter Kanal von extern zu einem internen Gerät aufgebaut werden darf. Aus diesem Grund ist für den jeweiligen Standort eine weitere Instanz eines Integrationsservers in der PDTZ neben der im produktiven Netzwerk notwendig. Dieser hat die Aufgabe, mit den externen Systemen und Datenbanken zu kommunizieren. Die angesprochenen Datenbanken werden im Abschnitt „Repository“ genauer beschrieben.

4.3 Repository

Ausgehend von den Anforderungen an den Schutz der patientenbezogenen Daten auf der einen Seite und der Notwendigkeit diese für eine Übertragung zur Verfügung zu stellen, werden zusätzliche Datenbanken als Puffer benötigt, die innerhalb des Modells und Projekts zur eindeutigen Bestimmbarkeit mit dem Begriff Repository bezeichnet werden.

Deutlich wird die Notwendigkeit durch die Betrachtung des Datentransfers zwischen den beteiligten Anwendungssystemen des krankenhausweiten Informationssystems. In aller Regel greift weder ein externes System noch der Integrationsserver selbst direkt und aktiv auf die Daten eines Anwendungssystems zu und auch die Abfrage einzelner Informationen wird oft nicht unterstützt.

Der Ablauf kann eher als ereignisgesteuert angesehen werden. Sobald Informationen in einem der beteiligten Anwendungssysteme entstehen, also neue Daten erfasst bzw. Modifikationen vorgenommen werden, werden diese Informationen aktiv gesendet. Dieses Push-Prinzip macht es nun erforderlich die anfallenden Datensätze für den Datenaustausch mit externen Teilnehmern zwischen zu speichern. Dieses Speichern erfolgt im Repository, einer Datenbank mit vordefinierten Strukturen, die sämtliche benötigten Daten speichert. Je nach Defini-

tion kann ein Vorhalten bestimmter Informationen zeitlich begrenzt werden, so dass lediglich für die Behandlung benötigte Daten verfügbar sind.

Trotz Aufbau einer Struktur mit DMZ und PDTZ ist es nicht sinnvoll, sämtliche Informationen innerhalb der PDTZ zu speichern. Lediglich Daten, die tatsächlich für die Übertragung freigegeben wurden, sollen das interne Netz verlassen. Diese Forderung führt zu einer zweistufigen Ausprägung des Repository. Innerhalb des internen Netzwerkes werden alle benötigten Nachrichten aller Patienten gespeichert. Mit Hilfe einer Oberfläche, die eine einfache Sicht auf die verfügbaren Daten realisiert, können nun einzelne bzw. durch Mehrfachselektion mehrere Datensätze bzw. Patienten selektiert und gleichzeitig zur Freigabe für den jeweiligen Kommunikationspartner markiert werden. Die dann so ausgewählten Daten werden in die zweite Datenbank übertragen und können über die Oberfläche von den zugelassenen Mitarbeitern der jeweiligen externen Institution eingesehen werden. Bis zu diesem Zeitpunkt werden keine Informationen zu den kooperierenden Einrichtungen übertragen.

4.4 Präsentation

Wie bereits in der Abhandlung des Repository angedeutet, wird eine einfache Oberfläche benötigt, die es den Mitarbeitern der externen Einrichtungen ermöglicht, auf die benötigten Informationen zuzugreifen. In einem vorgelagerten Schritt müssen die Patientendaten durch Mitarbeiter der behandelnden Klinik für die Zugriffe freigegeben werden. Es sind entsprechend zwei verschiedene Sichtweisen erforderlich, die den Anforderungen der Anwender genügt.

4.4.1 Interne Darstellung

Die Präsentation der Daten aus interner Sicht wird benötigt, um aus dem Pool aller Patientendaten, diejenigen zu selektieren, die einer kooperierenden Einrichtung zur Verfügung gestellt werden sollen. Dabei wählt der Mitarbeiter den bzw. die Patienten sowie die weiterbehandelnde Klinik aus. Die so markierten Datensätze werden in die zweite Stufe, also in das Repository in der PDTZ, überführt. Abhängig von der zuvor vereinbarten Konfiguration, werden sämtliche Informationen bzw. nur eine Auswahl konkreter Daten transferiert.

Die interne Darstellung lässt sich weiter unterteilen in die Funktionen Export, also dem Verfügbar machen der Daten für Externe, und Import. Letzterer entspricht einer Datenübernahme in die hauseigenen Systeme, so dass im weiteren Verlauf alle benötigten Daten innerhalb des Krankenhausinformationssystems zur Verfügung stehen.

4.4.2 Externe Darstellung

Für den Zugriff von außen wird in der DMZ ein Server benötigt, der die Oberfläche für den Zugriff auf die Daten in der PDTZ zur Verfügung stellt. Hier bekommt der Kommunikationspartner eine Ansicht aller relevanten Daten und hat auf der einen Seite die Möglichkeit lediglich Einblick zu nehmen, anderseits wird der Anwender in die Lage versetzt, die für ihn wichtigen Informationen oder alle dem Patienten zugehörigen Daten für eine Übertragung vorzumerken. Mit Abschluss dieser Aktivität wird durch den oben beschrieben Integrationsserver eine Verbindung über den VPN-Tunnel zur Gegenseite aufgebaut, und die Informationen werden in das Repository der korrespondierenden Einrichtung übertragen.

5 Gesamtaufbau

Die vorangestellten Abschnitte sollten die einzelnen Aspekte der Architektur beleuchten, die zugrunde liegende Idee verständlich machen und verdeutlichen, warum Kommunikation und Integration im Krankenhaus wichtig sind. Zusätzlich soll herausgestellt werden welche Gefahren, Probleme und Rahmenbedingungen vorliegen und wie damit umzugehen ist.

Im Folgenden werden der Gesamtaufbau eines sicheren Netzwerkes im Krankenhaus, und eine Ablaufbeschreibung des Datenweges anhand eines konkreten Szenarios aufgezeigt und beschrieben.

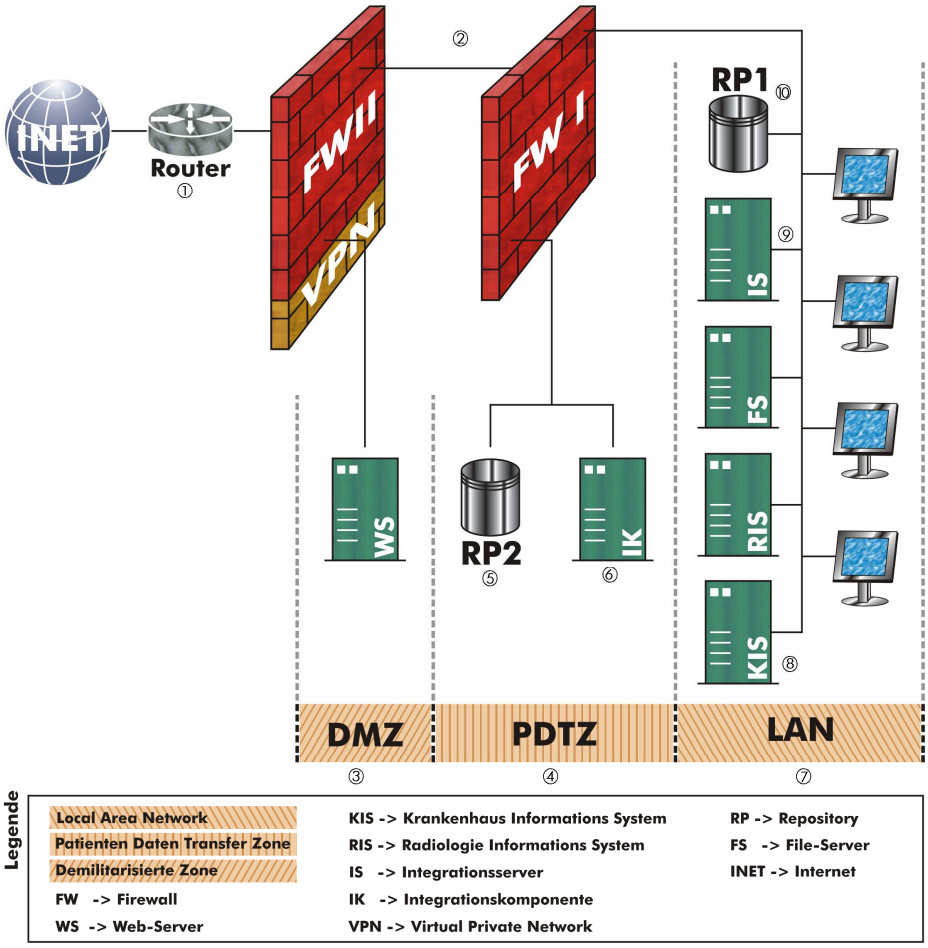


Abb. 8: Gesamtaufbau des Krankenhausnetzes

Mit der vorstehenden Grafik (Abb. 8) wird der Gesamtaufbau des sicheren Krankenhausnetzes für die Kommunikation mit externen Partnern dargestellt. Deutlich wird die Anbindung über den Router (1) eines Providers an das Internet sowie das zweistufige Firewallsystem (2). Der Webserver (WS), also die Visualisierungskomponenten in der DMZ (3) ist der einzige Rechner, welcher von extern mittels der VPN-Verbindung zugreifbar ist und lediglich diesem ist es möglich, die Anfragen von extern durch Zugriff auf die Daten in der PDTZ (4) zu beantworten. Die dort im Repository 2 (5) bereitgestellten Daten werden über die Integrationskomponente (6) mit dem Repository 1 (10) ausgetauscht. Das Repository 1 wiederum erhält seine Daten über den Integrationsserver (9) im LAN (7). Fileserver, Radiologie Informationssystem (RIS) und das Krankenhausinformationssystem (8) stehen beispielhaft für alle möglichen Primär- und Subsysteme innerhalb des produktiven Netzwerks.

Die nachstehenden Abschnitte gehen auf diese Zusammenstellung ausführlich ein.

Die Grundgedanken für jegliche sichere Kommunikation im Krankenhaus umfassen die Standpunkte, keine direkte Verbindung von außen ins interne, produktive LAN zuzulassen, Patientendaten besonders sicher zu behandeln und nicht permanent in einem Rechnerverbund der DMZ zu speichern. Darauf aufbauend lässt sich der Gesamtaufbau eines sicheren Netzes im Krankenhaus ableiten.

Der Internet-Zugang für die sichere Kommunikation mit anderen Krankenhäusern sollte vor allem von sonstigen Internet-Zugängen getrennt aufgebaut werden, um möglichst jede nicht benötigte Kommunikation zu deaktivieren und größtmögliche Sicherheit zu gewährleisten.

Ein Router steht für den Übergang zum Internet und verteilt und leitet jegliche Kommunikation ins Krankenhaus und heraus.

Ein Verbund aus zwei daran angeschlossenen Firewallsystemen mit integriertem VPN-Modul kontrolliert jeglichen Datenfluss in beide Richtungen. Mittels eines Regelwerks wird dieser gesteuert, eingegrenzt und wenn nötig unterbunden. Dadurch ist gewährleistet, dass kein Datenverkehr von oder zu ungewünschten Quellen entsteht.

Zwischen den beiden Firewallsystemen befindet sich die Demilitarisierte Zone (DMZ), die als geschützter Rechnerverbund fungiert und Dienste für die generelle Kommunikation sowohl dem internen, als auch dem externen Netz sicher zur Verfügung stellt.

Um den Grundsatz zu verfolgen, keine sensiblen Patientendaten in der DMZ zu speichern, wird hinter der zweiten Firewall die Patientendaten-Transfer-Zone (PDTZ), realisiert. Diese ist speziell für die Sicherheitsansprüche sensibler Patientendaten konzipiert und enthält neben dem Repository 2, der Datenbank in welcher die für die Übertrag an ein anderes Krankenhaus vorgemerkten Patientendaten gespeichert werden außerdem eine Integrationskomponente, welche den eigentlichen Datentransfer zu Partnerkliniken über eine Visualisierungskomponente ermöglicht.

Sowohl von der DMZ, als auch von der PDTZ entkoppelt existiert das produktive LAN. Dort existiert eine Fülle von Informationen und Daten, welche im KIS, dem gesamten Krankenhausinformationssystem mit allen Subsystemen, generiert werden. Dazu gehören beispielsweise persönliche Angaben zu Patienten, Befunde, Untersuchungs- und Operationsberichte, Medikation, Krankenakten etc.

Alle angefallenen Daten aus dem KIS werden von der Integrationskomponente, gesammelt und verarbeitet. Diese ist für das Zusammentragen, Umwandeln und Bereitstellen der notwendigen Informationen innerhalb des produktiven Netzwerks erforderlich. Alle Daten werden in einer speziellen Datenbank, dem Repository 1 zentral zwischengespeichert.

Wenn nun Daten für einen Kommunikationspartner zu Verfügung gestellt werden sollen, werden mittels der Integrationskomponente nun ausschließlich die für die Übertragung benötigten und vorher ausgewählten Daten aus dem Repository 1 in das Repository 2 der PDTZ kopiert.

Wenn Daten dort bereit liegen, wird der Kommunikationspartner automatisch benachrichtigt. Zuerst bekommt er über eine Präsentationskomponente in der DMZ einen Sichtzugriff auf die bereitgestellten Informationen und kann diese einsehen. Anschließend kann mittels Selektion ausgewählt werden, ob und welche Daten über eine sichere, verschlüsselte VPN-Verbindung übertragen werden sollen.

Dies minimiert den tatsächlichen Datenverkehr und erhöht die Sicherheit signifikant, indem nur die relevanten Daten übertragen werden.

6 Ablaufbeschreibung

Dieser Abschnitt beschreibt den kompletten Vorgang eines möglichen Datenaustausches in seiner zeitlichen Abfolge.

Vorausgesetzt wird dabei die beschriebene Infrastruktur bestehend aus einer sicheren Kommunikationsschicht mit Hilfe von Firewall, Einrichtung einer DMZ sowie PDTZ und weiteren Komponenten, die aus den Anforderungen der einzelnen Projekte hervorgehen.

Basis für den Datenaustausch ist das so genannte Data-Mining. Sämtliche patientenbezogenen Informationen werden in einem Repository gespeichert. Innerhalb des Hauses bedeutet dies, dass alle Daten, die von den angeschlossenen Systemen gesendet werden, neben den eigentlichen Zielsystemen auch dem Repository zugestellt werden.

Ein Mitarbeiter der Einrichtung meldet sich entsprechend seiner Zugriffsberechtigung an der internen Oberfläche des Transaktionssystems an. Durch Setzen von Filtern oder Direktauswahl konkreter Patienten wählt der Anwender die entsprechenden Patienten aus und ordnet diesen Datensätzen das Krankenhaus zu, welchem die Informationen bereitgestellt werden sollen. Nach Abschluss dieser Aufgabe werden lediglich die markierten Daten in die zweite Ebene des Repository überführt, einem Datenbanksystem in der PDTZ. Je nach Vereinbarung kann sogleich eine Nachricht an die jeweiligen Einrichtungen abgesetzt werden, die über das Bereitstellen der neuen Informationen informieren.

Der Anwender der kooperierenden Anstalt kann nun über die Präsentationsebene die bereitgestellten Daten einsehen und diese bei Bedarf für die Übernahme in das eigene Repository markieren. Durch die Integrationskomponenten werden die Informationen zwischen den beiden PDTZ transferiert. Auf diese Weise wird der tatsächliche Datentransfer auf das Notwendigste beschränkt, denn nur ausgewählte Patienteninformationen werden übertragen. Zum Zeitpunkt der Übertragung hat der Anwender die Möglichkeit zu bestimmen, ob

sämtliche Daten in das hauseigene KIS überführt werden sollen. Sollte diese Auswahl zu diesem Zeitpunkt nicht gemacht worden sein, kann auch später auf Basis der bereits übertragenen Daten dem System diese Anforderung bekannt gemacht werden, und eine entsprechende Funktion wird durch die Integrationskomponente getriggert.

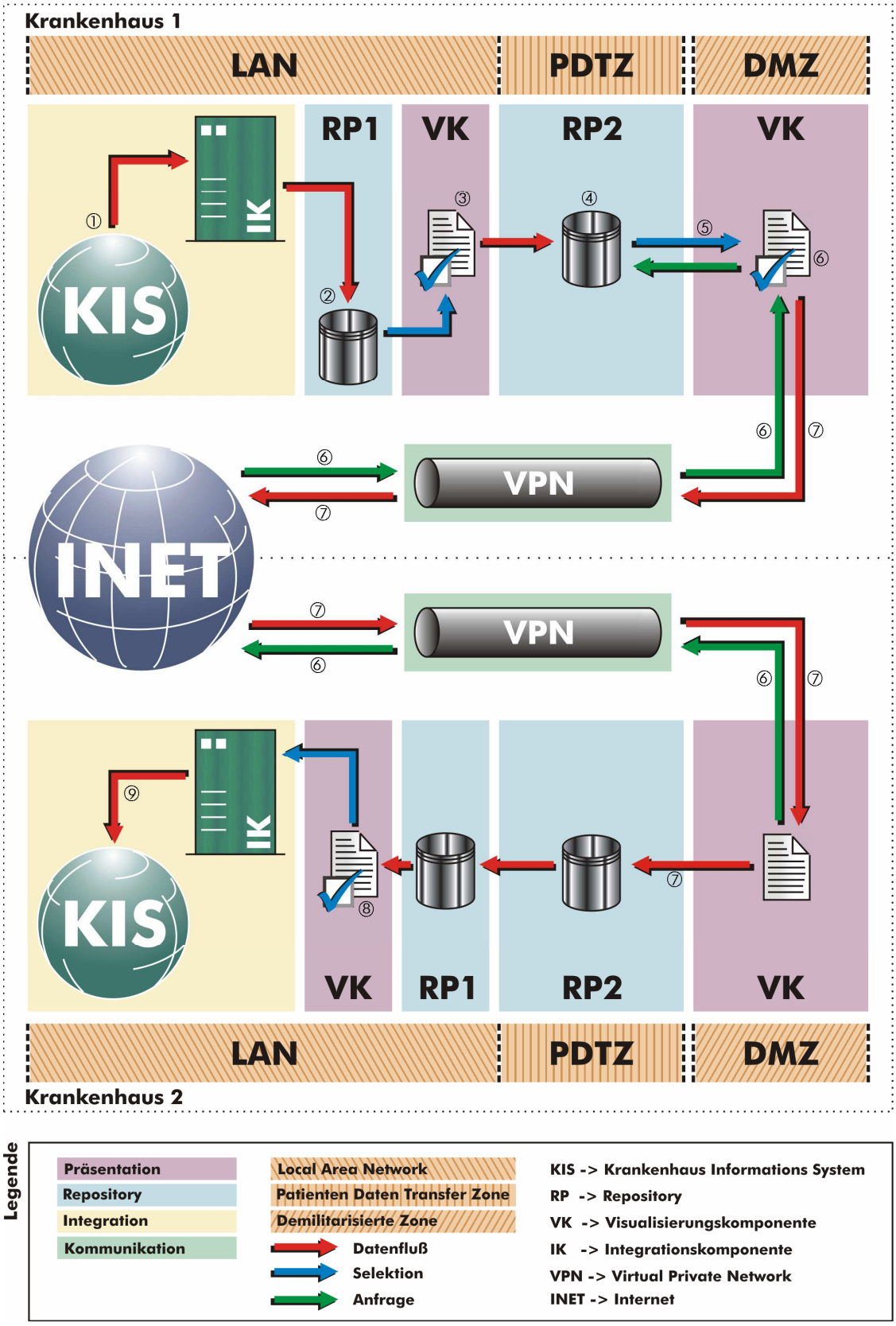


Abb. 9: Ablaufbeschreibung

Die vorstehende Darstellung (Abb. 9) präsentiert den gedachten Ablauf und skizziert einen möglichen Zugriff unter Berücksichtigung der gestellten Anforderungen an die sichere Kommunikation. Es werden zwei Krankenhäuser dargestellt, die beide über den dreistufigen Aufbau, also LAN, PDTZ und DMZ verfügen. Hervorzuheben ist, dass keine Anfrage von extern einen Einfluss auf den Datenfluss über die PDTZ, also in das LAN, hinaus ermöglicht.

Konkret erläutern die folgenden Absätze den Ablauf beispielhaft.

Zunächst nimmt das Krankenhaus 1 einen Patienten auf. Im Laufe von Untersuchungen werden Daten wie Röntgenbilder, Blutwertanalysen, Medikation, Arztbriefe usw. im Krankenhausinformationssystem (KIS) ermittelt.

Diese Daten werden vom KIS allen internen Systemen zur Verfügung gestellt, sowie zentral im RP 1 gespeichert.

Nun wird durch Analyse der Befunddaten festgestellt, dass eine Verlegung des Patienten in die kooperierende Fachklinik (Krankenhaus 2) indiziert ist.

Ein autorisierter Mitarbeiter des Krankenhaus 1 selektiert aus allen vorhandenen Daten über den Patienten die für die Weiterbehandlung relevanten Befunde. Diese werden in das RP2 in die PDTZ transferiert und für einen Sichtzugriff von außen über die Visualisierungskomponente freigegeben.

Die Fachklinik wird automatisch per eMail informiert, dass Daten für einen neuen Patienten vorliegen, kann diese einsehen und gegebenenfalls für die sichere Übertragung per VPN markieren.

Alle markierten Daten können nun zwischen den Kliniken übertragen werden. Mittels einer Visualisierungskomponente werden diejenigen Daten ausgewählt, welche in das hauseigene Netz übernommen werden sollen. Dort kann selektiert werden, welche der übernommenen Daten in das KIS eingegliedert werden

sollen. Dort werden sie von der Integrationskomponente (IK) weiterverarbeitet und allen internen Systemen zur Verfügung gestellt.

So stehen dem weiterbehandelnden Arzt alle Befunde und sonstigen Informationen über seine Patienten zur Verfügung.

7 Diskussion

Die Architektur, die im Rahmen dieser Arbeit geschaffen wurde, bietet den Institutionen im Gesundheitswesen eine Möglichkeit pragmatisch und kostengünstig eine Kommunikationsplattform zu erstellen. Die derzeitigen Anforderungen können damit erfüllt werden und bieten eine erhöhte Sicherheit sowie die Konsolidierung der verschiedenen Übertragungswege, die zurzeit im Einsatz sind. Eine Recherche in den einschlägigen Literaturdatenbanken und Suchmaschinen im medizinischen Bereich wurde durchgeführt. Dazu wurden unter anderem die Datenbanken von Medline, BMJ (British Medical Journal), NEMJ (The New England Journal of Medicine) und PubMed (Service der National Library of Medicine) abgefragt und genutzt. Als Ergebnis der Recherche kann zusammengefasst festgehalten werden, dass das vorliegende Konzept im Markt bisher noch nicht verfolgt wird. Betrachtet werden sehr wohl die einzelnen Aspekte, die in den verschiedenen Ebenen meines KIRP/V-Modells betroffen sind. Dabei geht es konkret um Datenformate für das Füllen und Übertragen von Informationen, die Gestaltung der Oberfläche zur Visualisierung über Web-Seiten und die Struktur der Datenbanken. Ebenfalls stark im Focus der Abhandlungen sind die Möglichkeiten zur Verschlüsselung auf der Kommunikationsebene. Die meist älteren Artikel beschäftigen sich beispielsweise mit Übertragungen mittels SSL (secure socket layer) und nicht wie im vorliegendem Konzept angedacht und empfohlen mittels VPN-Verbindungen.

Man stößt über die allgemeinen Internetsuchmaschinen (Google etc.) auf einige Anbieter, welche versuchen sich im Markt mit Lösungen für die Zuweiserbindung zu etablieren. Die dort erkennbaren Ansätze sind im Prinzip vergleichbar. Ausgehend von der zunächst komfortabel erscheinenden Ausgangssituation, auf die Befunddaten jederzeit im eigenen Krankenhausinformationssystem zugreifen zu können, wird externen Kommunikationsteilnehmern ein Client der jeweiligen Software zur Verfügung gestellt und der Zugriff auf die Daten ermöglicht. Der Anwender erhält dabei spezielle, eingeschränkte Rechte, arbeitet aber auf dem Primärsystem. Neben der Tatsache, dass die Installation des Clients beim Anwender (z.B. wegen der Wartbarkeit, Einspielen von Updates) proble-

matisch ist, ist genau dieser Ansatz, also externen direkten Zugriff in das produktive Netzwerk auf die Primärsysteme zu gestatten, äußerst bedenklich entsprechend den Anforderungen an die Sicherheit. Soll beispielsweise ein niedergelassener Arzt in einem Ballungsgebiet mit mehren Krankenhäusern Daten austauschen würde er von verschiedenen Anbieter die Software benötigen. Da eine Koexistenz der Clients auf einem Rechner mit großer Wahrscheinlichkeit zu Problemen führen würde, ist dieses Vorgehen sicher nicht sinnvoll. Aus wirtschaftlichen Erwägungen eines Anbieters mag das anders eingeschätzt werden. Neben den technischen Hürden ist ebenfalls die Bedienbarkeit der Software ein Problemfeld, da der Niedergelassene sich mit sämtlichen Clients auskennen müsste. In der Praxis hat dieses Vorgehen keinen Erfolg.

Des Weiteren wird es dann eine große Herausforderung, wenn außer den Daten aus dem KIS auch noch Informationen aus den Subsystemen benötigt werden (beispielsweise Röntgenbilder aus einem PACS, Laborwerte- und befunde aus einem Laborinformationssystem usw.).

In dem Zusammenhang der Zuweiserbindung werden neben den Patientendaten auch andere Informationen ausgetauscht, um die Bindung zwischen den Kommunikationspartnern zu erhöhen. Dabei könnten unter anderen Terminkalender, Informationen zu Behandlungspfaden und Fortbildungsveranstaltungen eine Rolle spielen. Bei dem Konzept der Nutzung der Clients der KIS-Hersteller sind solche Marketingaspekte nicht berücksichtigt.

Ein ganz anderer und wohl wesentlicher Ansatz sind die bereits angesprochenen zentralen Datenbanken oder aus Clinical Data Repositories (CDR[22]). Hierin sollen im Rahmen der Integrierten Versorgung vereinbarte Informationen für die Allgemeinheit, natürlich unter Berücksichtigung der jeweiligen Berechtigungen, zur Verfügung gestellt werden. Dahinter steckt die Idee zur Schaffung einer neutralen, herstellerunabhängigen Plattform.

[22] s.a. Glossar

Dieses Konzept wird sicher, wegen der großen Heterogenität im Gesundheitswesen nicht zu umgehen sein, jedoch sind die Schwachpunkte genauer unter die Lupe zu nehmen und diese nach Möglichkeit zu eliminieren bzw. zu minimieren. Zum einen wird ein Mechanismus benötigt, der dafür sorgt, dass die vereinbarten Informationen zu einem bestimmten Zeitpunkt in die zentrale elektronische Patientenakte (ePA) überführt werden. Ein Zugriff von extern soll aber unterbunden werden und die Abfrage von Daten auf den proprietären Strukturen der Anbietersoftware wird nicht umsetzbar sein.

In einem solchen Fall ist die vorliegende Architektur keine parallel zu verfolgende Idee noch ein Konkurrenzkonstrukt, sondern viel mehr eine notwendige Ergänzung zu den Anforderungen in der Integrierten Versorgung (IGV) und dem Aufbau zentraler Datenbanken, die mit Informationen aus den Institutionen im Gesundheitswesen bedient werden. Denn das, was aus Sicht dieser Anbieter oftmals mit „Infrastruktur“ bezeichnet wird, die bei diesen Projekten benötigt wird, wird vorausgesetzt. Dementsprechend muss jede Einrichtung für sich dafür sorgen, dass diese Voraussetzungen geschaffen werden.

Letztlich ist das Szenario immer gleich: es werden Daten aus dem administrativen und Abteilungssystemen benötigt. Diese sind in der Regel nicht zugreifbar sondern müssen über die besprochene Integrationskomponente abgegriffen werden. Damit ein späterer Zugriff oder Datentransfer stattfinden kann, müssen diese Daten in einer strukturierten Datenbank, dem Repository, zwischengespeichert werden. Daten, die nach außen kommuniziert werden sollen, müssen gefiltert werden und für die Übertragung bereitgestellt werden. Liegen diese Informationen dann in der Patientendaten-Transfer-Zone können sie, ähnlich dem beschriebenem Weg in der Ablaufbeschreibung nach dem Pull-Prinzip abgeholt werden oder nach Vereinbarung mit dem Betreiber des zentralen Archivsystems nach dem Push-Prinzip übertragen werden.

Wesentlichen Einfluss auf die Umsetzung dieses Konzeptes nehmen die Einführung der Versichertenkarte und der damit verbunden „Health Professional

Card“ (HPC), welche den Mitarbeitern in Heilberufen zur Verfügung gestellt wird. Diese Karte wird alleine oder in Kombination mit der Versichertenkarte den Zugriff auf Daten steuern und gleichzeitig ein Zertifikat beinhalten, welches die Berechtigung des Besitzers überprüft. Grundsätzlich ist auf Grundlage meines KIRP/V-Modells eine Integration dieser Verschlüsselung und Zugriffsteuerung unproblematisch.

8 Ausblick

Mit der vorliegenden Arbeit steht den Krankenhäusern und auch anderen Institutionen im Gesundheitswesen ein Konzept zur Verfügung, mit dem die gegenwärtigen Anforderungen unter pragmatischen und kostenrelevanten Gesichtspunkten erfüllt werden können.

Im Abschlussbericht zur Gesundheitskarte und Telematik-Infrastruktur (Teletrust 2004) wird empfohlen, mit einer pragmatischen und robusten Lösung zu starten, die ein hohes Einsparpotential ermöglicht. Es muss jedoch eine Migration zu neueren Techniken und die Einbindung weiterer Funktionalitäten bzw. Applikationen mit geringem finanziellem und organisatorischem Aufwand möglich sein. Eine Harmonisierung in Europa sollte unter den gleichen Aspekten möglich sein.

„Erst durch eine umfassende Vernetzung im Gesundheitswesen würden die Prozesse so effizient, dass technologische Innovationen in den Praxen und Krankenhäusern finanzierbar werden“ (Ärzte Zeitung 2005).

Die eigentlichen Herausforderungen gehen weit über die zurzeit vereinbarten Basisdienste hinaus. Langfristiges Ziel ist eine europäische Lösung, die entsprechende Standardisierung, zumindest eine größtmögliche Interoperabilität zulässt (DIMDI 2004).

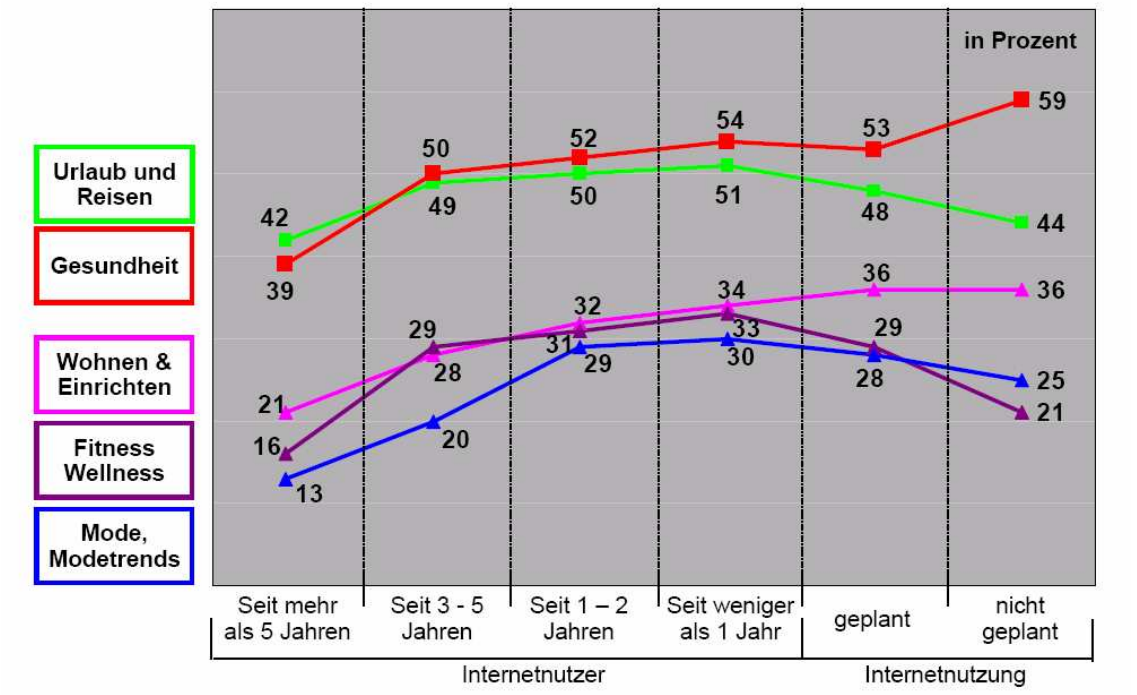
„Telematik, ganzheitlich betrachtet, zeigt auf, dass moderne Informations- und Kommunikationstechnologie sehr wohl geeignet ist, Lösungsansätze für Transparenz, Integration und Vernetzung zu bieten. Strebt man eine weitere Entwicklung der medizinischen Leistungsfähigkeit unter gleichzeitiger Kostenbegrenzung an, so ist dies kaum ohne den Einsatz telematischer Lösungen erreichbar“ (Roland Berger Beratung 1997).

Das vorliegende Konzept ermöglicht es bereits jetzt, einen sicheren Datenaustausch zwischen den Teilnehmern im Gesundheitswesen zu gewährleisten und ist durch die große Flexibilität prinzipiell als Ergänzung zu den geplanten, internationalen Strategien zu sehen. Denn beinahe unabhängig von der tatsächlichen Struktur bleiben die grundlegenden Anforderungen doch immer gleich. Es wird eine sichere Kommunikationsstruktur nach außen benötigt, der Zugriff von extern auf den gesamten Datenbestand ist und bleibt unerwünscht, so dass für einen Datentransfer, wohin auch immer, das Extrakt der Daten für den Austausch vorgehalten werden muss. Diese Informationen soll entweder in einem standardisierten Format vorliegen, oder jedoch mit Hilfe von Integrationswerkzeugen anderen Applikationen zugänglich gemacht werden. Nicht zuletzt wird für diverse administrative Arbeiten eine Oberfläche benötigt.

Die Investitionen, die eine Institution für die hier beschriebene Plattform tätigen muss, sind also nicht verloren. Vielmehr wird eine solche Infrastruktur ohnehin benötigt und eine rasche Umsetzung kann der Einrichtung einen großen Vorteil im zunehmenden Wettbewerb verschaffen und gleichzeitig eine Kostenersparnis bringen.

Neben der Kommunikation zwischen den Teilnehmern wird auch Zugriff des Patienten auf seine Daten diskutiert und scheint auch sinnvoll.

Die folgende Grafik zeigt, dass das Informationsbedürfnis an Gesundheitsthemen im Internet zunimmt.



Basis: Bundesrepublik Deutschland, Bevölkerung 14 – 64 Jahre
Quelle: Allensbacher Computer- und Telekommunikations-Analyse, ACTA 2002

Abb. 17 Informationsbedürfnis

Warum sollte es dem Patienten, als Herr seiner Daten, nicht ermöglicht werden, durch einheitliche und sichere Zugriffsverfahren von seinem Recht Gebrauch zu machen, seine Daten einzusehen? Viele Parallelen zum Homebanking lassen sich erkennen, wenn auch geregelt werden muss, dass abhängig von bestimmten Diagnosen zum Schutz des Patienten, nicht alle Informationen angezeigt werden dürften.

9 Zusammenfassung

Im Hinblick der erweiterten Anforderungen auf den sicheren Datenaustausch im Rahmen der Integrierten Versorgung, ist der Aufbau einer entsprechenden Infrastruktur eine wesentliche Voraussetzung, um den datenschutzrechtlichen Anforderungen Rechnung zu tragen.

Aus diesen speziellen Anforderungen heraus hat sich der Begriff Patientendaten-Transfer-Zone (PDTZ) bei der konzeptuellen Betrachtung der Sicherheitsstrategie im Gesundheitswesen gefestigt. Die PDTZ bezeichnet eine zusätzliche Schutzzone in der Übertragungsarchitektur, die neben der DMZ (demilitarisierten Zone) als weitere Ebene den sicheren Datenaustausch gewährleistet. Der Grundgedanke, der sich dahinter verbirgt, ist es nach Möglichkeit jeglichen direkten Kanal zwischen dem öffentlichen Netz und dem produktivem Netzwerk zu unterbinden.

Für sämtlichen Datentransfer sollte immer der Gedanke einer Schleuse verfolgt werden. Eingehende Informationen treffen zunächst in einer DMZ ein und werden von dort weitergeleitet. Nun würde von der Idee her die DMZ, sei sie an einer weiteren Netzwerkkarte der ersten Firewall oder als Zone zwischen den beiden Firewallsystemen realisiert, die Anforderung, keine direkte Verbindung ins interne produktive Netzwerk zuzulassen, erfüllen. Jedoch steht die nachvollziehbare Forderung im Raum, nach der in der DMZ keine Patientendaten permanent gespeichert werden dürfen. Für einen dateibasierten Austausch könnte dies bereits problematisch sein, denn es ist nicht definiert, wie groß der Zeitraum zwischen Einstellen der Daten und Abholung durch interne Systeme sein darf. Um größtmögliche Sicherheit zu erreichen wird ein zusätzlicher, sicherer Bereich benötigt, der nicht mehr als DMZ bezeichnet werden kann, jedoch auch noch nicht dem internen produktiven Netzwerk zugehörig ist. Dieser Bereich der PDTZ stellt prinzipiell keine zusätzlichen Anforderungen an die eingesetzten Sicherheitskomponenten, sondern entspricht parallel zur DMZ lediglich einer entsprechenden Konfiguration, welche allerdings eine erhebliche Steigerung der Datensicherheit hervorbringt.

10 Literaturverzeichnis

1. Albert, J., David, D., Langerfeld, C. (2004):
   Management-Papier „Pseudonymisierung / Anonymisierung“
   Köln: Gesellschaft für Versicherungswissenschaft und – gestaltung.
   auch: http://atg.gvg-koeln.de/xpage/objects/pseudonymisierung/docs/5/files/MP040316.pdf

2. Ärzte Zeitung: Vernetzung bringt großen Schub, 2005, Online-Publikation;
   http://www.aerztezeitung.de/docs/2005/02/23/033a1501.asp?cat

3. van Bemmel, J.H., Musen, M.A. (1997):
   Handbook of Medical Informatics. 1. Auflage
   Heidelberg: Springer-Verlag; S. 67.

4. Beske, F., Brecht, J., Reinkemeier, A.-M. (1993):
   Das Gesundheitswesen in Deutschladn. 1. Auflage
   Köln: Deutscher Ärzte Verlag; S. 105.

5. Boeske; M., Custodis, F. ; Goetz, C. (2003):
   Managementpapier zur Elektronischen Patientenakte
   Köln: Gesellschaft für Versicherungswissenschaft und –gestaltung Aktionsforum Telematik im Gesundheitswesen
   http://atg.gvg-koeln.de/xpage/objects/patientenakte/docs/1/files/MSt1_Vers4-1_oeffentl-Komment_04072003.pdf

6. Buchholz, E. (1988):
Unser Gesundheitswesen. 1. Auflage
Heidelberg: Springer-Verlag; S. 13.

7. Bundesamt für Sicherheit in der Informationstechnik (2003):
BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit
http://www.bsi-fuer-buerger.de/down/sinet.pdf, 2003

8. Dietzel, G., Riepe, C. Modernizing healthcare in Germany by introducing the eHealthcard (2004) Federal Ministry for Health and Social Security
http://www.dimdi.de/de/ehealth/literatur/sim52-18-22-germany.pdf

9. DIMDI- Deutsches Institut für Medizinische Dokumentation und Information:
Die elektronische Gesundheitskarte – Ziele, 2004
http://www.dimdi.de/de/ehealth/karte/basisinformation/ziele/index.htm

10. DIMDI- Deutsches Institut für Medizinische Dokumentation und Information:
Die elektronische Gesundheitskarte – Umsetzung und Ausblick, 2004
http://www.dimdi.de/de/ehealth/karte/basisinformation/umsetzung/index.htm

11. Goetz, C.; Sembritzki, J. (1998):
Kryptographische Verfahren im Gesundheits- und Sozialwesen in Deutschland. Erfurt: TeleTrust Deutschland e.V.; S. 16.

12. Helmbrecht, U.: Leitfaden IT-Sicherheit – IT-Grundschutz kompakt. 2004, Online-Publikationen; http://www.bsi.bund.de/gshb/Leitfaden/GS-Leitfaden.pdf

13. Krüger-Brand, H.. (2003):
E-Health und E-Commerce in der Praxis: Mehr Qualität und Effizienz.
Deutsches Ärzteblatt 100, Ausgabe 11 Seite A-683 / B-585 / C-549

14. Lauterbach, K. ; Lindlar, M.: Informationstechnologien im Gesundheitswesen (Gutachten), Bonn: 1999 Friedrich-Ebert-Stiftung
http://www.medizin.uni-koeln.de/kai/igmg/gatm/ga_tm_99.pdf

15. Rohleder, B., Brüning, M., Hollmann, A.: Einführung einer Telematik-Architektur im deutschen Gesundheitswese, Expertise, 2003
http://www.dimdi.de/de/ehealth/literatur/telematik_expertise.pdf

16. Roland Berger Beratung (1997):
Telematik im Gesundheitswesen - Perspektiven der Telemedizin in Deutschland – für Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie und Bundesministerium für Gesundheit
http://www.dimdi.de/de/ehealth/literatur/roland_berger_studie.zip

17. Teletrust Deutschland e.V. (2004):
Abschlußbericht zu GuT - Gesundheitskarte und Telematik-Infrastruktur
http://www.teletrust.de/dokumente/gut_uag3aii-bericht.pdf

18. Trill, R. (2002):
Informationstechnologie im Krankenhaus. 1.Auflage
Neuwied: Hermann Luchterhand Verlag; S. 88.

19. Veit, T.: Firewallsysteme: Konzeption – Implementation – Audit. BSI 2000,
Online-Publikationen: http://www.bsi.bund.de/fachthem/sinet/vt_071.htm

11 Verwendete Abkürzungen

ASP	Application Service Provider, Rechenzentrumsbetrieb
BSI	Budesamt für Sicherheit in der Informationstechnik
CC EAL	Common Criteria Evaluation Assurance Level
DMZ	Demilitarisierte Zone
GMG	Gesetz zur Modifizierung der gesetzlichen Krankenversicherung
IGV	Integrierte Versorgung
ITSEC	International Trusted System Evaluatoin Criteria
KIS	Krankenhausinformationssystem
NAT	Network address translation
PAT	Port address translation
PDTZ	Patientendaten-Transfer-Zone
SDSL	Symmetric Digital Subscriber Line
ADSL	Asymmetric Digital Subcriber Line
VPN	Virtuelles Privates Netz
LAN	Local Area Network

12 Glossar

CDR
Clinical Data Repository

zentrale Datenbank zur Sammlung von relevanten Patienteninformationen im Zusammenhang des Betriebs in Rechenzentren.

DDV

Die Digitale Direktverbindung ist die Bezeichnung einer Standleitung, also einer Punkt-zu-Punkt-Verbindung zwischen zwei Standorten. Durch sichere kryptografische Verfahren werden diese zunehmend durch VPN-Anbindungen abgelöst.

DMZ

Die Demilitarisierte Zone, auf deutsch auch entmilitarisierte Zone, bezeichnet eine definierte Zone in der Sicherheitsstruktur zwischen zwei Netzen. Während der Zugriff auf lokale Netze durch Externe verboten wird, sind Computer in der DMZ speziell für den Zugriff aus beiden, dem internen und externen Netz, konzipiert.

DSL

Es werden synchrone und asynchrone Digital Subscriber Lines unterschieden. Diese Technik ermöglicht einen hohen Datendurchsatz auf einer gewöhnlichen 2-Drahttechnik. Beim synchronen Verfahren (SDSL) ist die Datenrate in beiden Richtungen gleich hoch, beim asynchronen (ADSL) beträgt der Upload-Durchsatz nur einen Bruchteil der Download-Richtung. SDSL ist für den Datenaustausch mit externen Kommunikationspartnern besser geeignet.

Firewall	Einrichtung am Netzübergang zur Abwehr unerlaubter Zugriffe und Steuerung von Zugangsberechtigungen. Oftmals mit integrierter VPN-Funktionalität.
Flatrate	Leitungen ins Internet werden entweder nach Volumen, also übertragender Datenmenge oder pauschal ohne Übertragungslimit über die so genannte Flatrate berechnet.
IGV	Die Integrierte Versorgung (IGV, auch IV abgekürzt) ist ein gesetzlich verankerter Begriff, der eine sektorübergreifende Zusammenarbeit der Einrichtungen des Gesundheitswesen vorschreibt, welche nicht zwingend elektronisch sein muss.
Integrationsserver	Ein Integrationsserver, oft auch als Schnittstellenserver bezeichnet, dient derm Austausch von Daten zwischen verschiedenen Anwendungssystemen. Die Informationen werden über verschiedene Verfahren transportiert und für die Verwendung im anderen System, der dortigen Darstellung entsprechend, modifiziert.
IP-Adresse	Eine eindeutige Adresse im Internet Protokoll, durch den ein einzelner Computer identifiziert werden kann. Bei der Einwahl bei einem Provider werden entweder statische IP-Adressen, die immer wieder dem gleichen Kunden zugeordnet werden, vergeben oder es wird mit einer dynamischen Vergabe gearbeitet. Der Kunde erhält dabei mit jeder Anmeldung eine andere Adresse aus dem Adressvorrat des Anbieters.

Java-Applet	Ein Java-Applet ist ein kleines Programm, welches in Web-Seiten eingebettet Funktionen auf dem lokalen Rechner ausführen kann. Wegen dieser Möglichkeit, werden diese oftmals auch zum Ausspähen oder Zerstören von Daten auf lokalen Datenträgern missbraucht.
KIS	Mit Krankenhausinformationssystem wird im Gesundheitswesen, entgegen der normalen Verwendung des Begriffs Informationssystem, meist nicht die Gesamtheit aller Anwendungssysteme bezeichnet, sondern viel mehr das administrative, patientenführende Primärsystem
Kommunikationsserver	Ein Kommunikationsserver bezeichnet einen Computer, der Funktionen für die Nutzung von Internetdiensten zur Verfügung stellt, wie beispielsweise eMail, Web-Seiten, Zugrifssteuerung aucf das Internet, sowie einen Zwischenspeicher (Proxy).
LAN	Das LAN (local area network) bezeichnet das lokale Netzwerk, also z.B. innerhalb eines Krankenhauses.
MPI	Der Master-Patient-Index dient der eindeutigen Identifizierung von Patientendaten und wird benötigt, da einrichtungsübergreifend verschiedene Nummernkreise genutzt werden. Mit Einführung einer eindeutigen Patienten-ID durch die Krankenversichertenkarte rückt diese Problematik auf lange Sich in den Hintergrund.
PDTZ Patientendaten-Transferzone	Spezieller Bereich in der Sicherheitsinfrastrukur für den Datentransfer schützenswerter Informationen.
Viruswall	Einrichtung am Übergang zum Internet zur Abwehr

	von Viren, Trojanern etc., bevor diese auf die Arbeitsstation und Server gelangen können.
VPN	Ein VPN (Virtuelles Privates Netzwerk) bezeichnet verschlüsselte Verbindungen zur Vernetzung von Standorten über unsichere Netze (z.B. Internet)

Danksagungen

Bedanken möchte ich mich bei Herrn Priv.-Doz. Dr. Rolf R. Diehl, der mich bei der Erstellung der vorliegenden Arbeit betreut hat und für Diskussionen auch am Telefon und per
eMail zur Verfügung stand.

Besonderer Dank gilt meinen Eltern, die mir den Weg bis zur Erstellung einer solchen Arbeit überhaupt ermöglicht haben sowie meiner Familie, die mir für die benötigte Zeit den Rücken frei gehalten und mich immer wieder ermuntert hat.

Mein Dank gilt auch allen anderen Gesprächspartnern, die in einzelnen Gesprächen den Inhalt meiner Arbeit geschärft haben.

Curriculum Vitae

Vorname, Name:		Thomas Jäschke, wohnhaft in Dortmund
Geburtsdatum und -ort:		22. April 1968 in Gelsenkrichen
Staatsangehörigkeit:		Deutsch
Familienstand:		langfristige Partnerschaft
Kinder		Verena Nicole, geb. 09. Mai 1999 Linus Ferdinand, geb.11. Juni 2001 Justus Karl, geb. 30. Oktober 2004
Eltern:		Paul Ulrich Jäschke, Marie-Luise Jäschke, geb. Biebricher,
Geschwister:		Thorsten Jäschke, geb. 21.April 1970
Schulausbildung:	1974 – 1978	Grundschulen in Gelsenkirchen und Essen
	1978 – 1984	Bertha-von-Suttner Realschule, Essen Mittlere Reife
	1984 - 1987	Helmholz-Gymnasium, Essen Allgemeine Hochschulreife
Zivildienst:	01.03.88 - 31.10.89	Alfried Krupp von Bohlen und Halbach Krankenhaus im Pflegebereich
Studium:	01.10.1989 – 30.03.1995	Studium der Informatik mit Schwerpunkt theoretischer Medizin, Universität Dortmund
Tätigkeiten:	31.12.89- 30.06.94	Erwerbsbehinderten-Arbeitsstätte als Altenpflegehelfer als Aushilfe
	17.06.91 - 30.04.92	Universität-GH Essen, als studentische Hilfskraft in der Onkologie für statistische Auswertungen
	01.05.95 – 30.04.96	Alfried Krupp von Bohlen und Halbach Krankenhaus als Systemanalytiker
	01.05.96 – 31.03.99	SMS Dataplan GmbH & Co. KG als Projektleiter, Anwendungsberater und im technischem Service
	seit 01.01.99	Geschäftsführer der ISPro GmbH